II

(Actos no legislativos)

REGLAMENTOS

REGLAMENTO DE EJECUCIÓN (UE) 2016/799 DE LA COMISIÓN

de 18 de marzo de 2016

por el que se ejecuta el Reglamento (UE) n.º 165/2014 del Parlamento Europeo y del Consejo, que establece los requisitos para la construcción, ensayo, instalación, funcionamiento y reparación de los tacógrafos y de sus componentes

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 165/2014 del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, relativo a los tacógrafos en el transporte por carretera ([1]), y en particular su artículo 11 y su artículo 12, apartado 7,

Considerando lo siguiente:

(1) El Reglamento (UE) n.º 165/2014 ha introducido el tacógrafo digital de segunda generación denominado tacógrafo inteligente, que incluye una conexión con el dispositivo GNSS (sistema mundial de radionavegación por satélite), un dispositivo de comunicación a efectos de teledetección temprana y una interfaz con los sistemas de transporte inteligentes. Deben establecerse las especificaciones de los requisitos técnicos para la fabricación de tacógrafos inteligentes.

(2) El dispositivo de teledetección temprana establecido por el artículo 9, apartado 4, del Reglamento (UE) n.º 165/2014 debe transmitir a un agente de control en carretera los datos del tacógrafo digital y la información relativa a los pesos y pesos por eje de todo el conjunto del vehículo (tractores y remolques o semirremolques), de conformidad con la Directiva 96/53/CE del Parlamento Europeo y del Consejo ([2]). De este modo, las autoridades de control podrán efectuar una comprobación rápida y eficaz de los vehículos, con menos dispositivos electrónicos en la cabina del vehículo.

(3) De conformidad con la Directiva 96/53/CE, el dispositivo de teledetección temprana debe utilizar las normas CEN DSRC ([3]) a que se refiere dicha Directiva, en la banda de frecuencias de 5 795-5 805 MHz. Toda vez que dicha banda de frecuencias se utiliza también en el telepeaje, y a fin de evitar interferencias entre las aplicaciones de peaje y de control, los controladores no deben utilizar el dispositivo de teledetección temprana en un área de peaje.

(4) Con el tacógrafo inteligente deben introducirse nuevos mecanismos de seguridad para mantener el nivel de seguridad del tacógrafo digital, a fin de corregir los actuales puntos vulnerables en materia de seguridad. Uno de esos puntos vulnerables es la ausencia de fechas de expiración de los certificados digitales. Con el fin de respetar las mejores prácticas en materia de seguridad, se recomienda evitar el uso de certificados digitales sin fecha de expiración. El período de validez operativa normal de las unidades instaladas en vehículos debe ser de quince años, a partir de la fecha de emisión de los certificados digitales de dichas unidades. Las unidades instaladas en vehículos deben ser reemplazadas al concluir el período de validez.

([1]) DO L 60 de 28.2.2014, p. 1.
([2]) Directiva 96/53/CE del Consejo, de 25 de julio de 1996, por la que se establecen, para determinados vehículos de carretera que circulan en la Comunidad, las dimensiones máximas autorizadas en el tráfico nacional e internacional y los pesos máximos autorizados en el tráfico internacional (DO L 235 de 17.9.1996, p. 59).
([3]) Normas de comunicaciones dedicadas de corto alcance del Comité Europeo de Normalización (CEN) EN 12253, EN 12795, EN 12834, EN 13372 e ISO 14906.

(5) El suministro de información fiable y segura sobre la localización constituye un elemento esencial del buen funcionamiento de los tacógrafos inteligentes. Por tanto, conviene garantizar su compatibilidad con los servicios de valor añadido prestados por el programa Galileo, según lo dispuesto en el Reglamento (UE) n.º 1285/2013 del Parlamento Europeo y del Consejo ([1]), a fin de mejorar la seguridad del tacógrafo inteligente.

(6) De conformidad con el artículo 8, apartado 1, el artículo 9, apartado 1, y el artículo 10, apartados 1 y 2, del Reglamento (UE) n.º 165/2014, los mecanismos de seguridad introducidos por dicho Reglamento deben aplicarse 36 meses después de la entrada en vigor de los actos de ejecución necesarios con el fin de permitir a los fabricantes el desarrollo de la nueva generación de tacógrafos inteligentes, y recibir de las autoridades competentes sus certificados de homologación.

(7) De conformidad con el Reglamento (UE) n.º 165/2014, los vehículos matriculados por primera vez en un Estado miembro 36 meses después de la entrada en vigor del presente Reglamento de la Comisión deben estar equipados con un tacógrafo inteligente que cumpla los requisitos en él contenidos. En cualquier caso, todos los vehículos que circulen en un Estado miembro distinto de su Estado miembro de matriculación deben estar equipados con un tacógrafo inteligente que cumpla los requisitos quince años después de la fecha de aplicación de estos.

(8) El Reglamento (CE) n.º 68/2009 de la Comisión ([2]) permitió, durante un período transitorio que finalizó el 31 de diciembre de 2013, la utilización de un adaptador para hacer posible la instalación de tacógrafos en vehículos de tipo M1 y N1. Debido a dificultades técnicas relacionadas con la búsqueda de una alternativa a la utilización del adaptador, los expertos de la industria del automóvil y del tacógrafo, junto con la Comisión, llegaron a la conclusión de que no era viable ninguna solución alternativa al adaptador que no supusiera un coste elevado para el sector, que sería desproporcionado en relación con el tamaño del mercado. Por lo tanto, debe autorizarse por tiempo indefinido la utilización de un adaptador en vehículos de tipo M1 y N1.

(9) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité a que se refiere el artículo 42, apartado 3, del Reglamento (UE) n.º 165/2014.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Articulo 1

Objeto y ámbito de aplicación

1. El presente Reglamento establece las disposiciones necesarias para la aplicación uniforme de los siguientes aspectos en relación con los tacógrafos:

a) registro de la posición del vehículo en determinados puntos durante el período de trabajo diario del conductor;

b) teledetección temprana de posibles manipulaciones o usos indebidos del tacógrafo inteligente;

c) interfaz con los sistemas de transporte inteligentes;

d) requisitos técnicos y administrativos para los procedimientos de homologación de los tacógrafos, incluidos los mecanismos de seguridad.

2. La construcción, ensayo, instalación, inspección, funcionamiento y reparación de los tacógrafos inteligentes y sus componentes deberán cumplir los requisitos técnicos establecidos en el anexo 1C del presente Reglamento.

3. Los tacógrafos distintos de los tacógrafos inteligentes seguirán teniendo que cumplir, en lo que se refiere a las condiciones de construcción, ensayo, instalación, inspección, funcionamiento y reparación, los requisitos establecidos en el anexo 1 o el anexo 1B del Reglamento (CEE) n.º 3821/85 del Consejo ([3]), según proceda.

([1]) Reglamento (UE) nº 1285/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, relativo al establecimiento y la explotación de los sistemas europeos de radionavegación por satélite y por el que se derogan el Reglamento (CE) nº 876/2002 del Consejo y el Reglamento (CE) nº 683/2008 del Parlamento Europeo y del Consejo (DO L 347 de 20.12.2013, p. 1).

([2]) Reglamento (CE) nº 68/2009 de la Comisión, de 23 de enero de 2009, por el que se adapta por novena vez al progreso técnico el Reglamento (CEE) nº 3821/85 del Consejo relativo al aparato de control en el sector de los transportes por carretera (DO L 339 de 24.1.2009, p. 3).

([3]) Reglamento (CEE) nº 3821/85 del Consejo, de 20 de diciembre de 1985, relativo al aparato de control en el sector de los transportes por carretera (DO L 370 de 31.12.1985, p. 8).

4. De conformidad con el artículo 10 *quinquies* de la Directiva 96/53/CE del Parlamento Europeo y del Consejo, el dispositivo de teledetección temprana transmitirá asimismo los datos sobre peso facilitados por un sistema de pesaje a bordo, con miras a la pronta detección de fraudes.

Articulo 2

Definiciones

A efectos del presente Reglamento, serán de aplicación las definiciones establecidas en el artículo 2 del Reglamento (UE) n.º 165/2014.

Asimismo, se entenderá por:

1) «tacógrafo digital» o «tacógrafo de primera generación»: un tacógrafo digital distinto de un tacógrafo inteligente;

2) «dispositivo GNSS externo»: la instalación que contiene el receptor GNSS cuando la unidad instalada en el vehículo no sea una unidad única, así como otros componentes necesarios para proteger la comunicación de los datos de posición al resto de la unidad instalada en el vehículo;

3) «expediente del fabricante»: la documentación completa, en formato electrónico o en papel, que contiene toda la información facilitada por el fabricante o su agente a la autoridad de homologación a efectos de la homologación de un tacógrafo o de uno de sus componentes, incluidos los certificados a que se refiere el artículo 12, apartado 3, del Reglamento (UE) n.º 165/2014, los resultados de los ensayos definidos en el anexo 1C del presente Reglamento, así como dibujos, fotografías y demás documentos pertinentes;

4) «expediente de homologación»: el expediente del fabricante, en formato electrónico o en papel, acompañado de los demás documentos añadidos por la autoridad de homologación a dicho expediente durante el desempeño de sus funciones, incluido, al finalizar el proceso de homologación, el certificado de homologación de tipo CE del tacógrafo o de uno de sus componentes;

5) «índice del expediente de homologación»: el documento que indica el contenido numerado del expediente de homologación, identificando todas sus partes pertinentes; el formato de dicho documento distinguirá las sucesivas etapas del proceso de homologación de tipo CE, incluidas las fechas de las revisiones y actualizaciones del expediente;

6) «dispositivo de teledetección temprana»: el equipo de la unidad instalada en el vehículo que se utiliza para llevar a cabo controles selectivos en carretera;

7) «tacógrafo inteligente» o «tacógrafo de segunda generación»: un tacógrafo digital que cumple lo dispuesto en los artículos 8, 9 y 10 del Reglamento (UE) n.º 165/2014, así como en el anexo 1C del presente Reglamento;

8) «componente del tacógrafo» o «componente»: cualquiera de los elementos siguientes: la unidad instalada en el vehículo, el sensor de movimiento, la tarjeta de tacógrafo, la hoja de registro, el dispositivo GNSS externo y el dispositivo de teledetección temprana;

9) «autoridad de homologación»: la autoridad de un Estado miembro competente para llevar a cabo la homologación del tacógrafo o de sus componentes, el proceso de autorización, la expedición y, en su caso, la retirada de los certificados de homologación, actuando como punto de contacto con las autoridades de homologación de los demás Estados miembros y asegurándose de que los fabricantes cumplen sus obligaciones relativas a la conformidad con los requisitos del presente Reglamento.

Articulo 3

Servicios basados en la localización

1. Los fabricantes velarán por que los tacógrafos inteligentes sean compatibles con los servicios de localización prestados por Galileo y por el sistema europeo de navegación por complemento geoestacionario (EGNOS).

2. Además de los sistemas a que se refiere el apartado 1, los fabricantes podrán también optar por garantizar la compatibilidad con otros sistemas de navegación por satélite.

Articulo 4

Procedimiento de homologación de los tacógrafos y de los componentes del tacógrafo

1. El fabricante o su mandatario presentará la solicitud de homologación de un tacógrafo, o de alguno de sus componentes, o grupo de componentes, a las autoridades de homologación designadas por cada Estado miembro. La solicitud consistirá en un expediente del fabricante que contenga la información sobre cada uno de los componentes en cuestión, así como, en su caso, los certificados de homologación de los demás componentes necesarios para completar el tacógrafo, junto con cualquier otro documento pertinente.

2. Un Estado miembro concederá la homologación a todo tacógrafo, componente o grupo de componentes que se ajuste a los requisitos administrativos y técnicos a que se refiere el artículo 1, apartados 2 o 3, según proceda. En tal caso, la autoridad de homologación expedirá al solicitante un certificado de homologación que deberá ajustarse al modelo establecido en el anexo II del presente Reglamento.

3. La autoridad de homologación podrá solicitar al fabricante o a su mandatario que facilite cualquier información adicional.

4. El fabricante o su mandatario pondrá a disposición de las autoridades de homologación, así como de las entidades responsables de la expedición de los certificados mencionadas en el artículo 12, apartado 3, del Reglamento (UE) n.º 165/2014, tantos tacógrafos o componentes del tacógrafo como sean necesarios para poder llevar a cabo de forma satisfactoria el procedimiento de homologación.

5. Cuando el fabricante o su mandatario solicite la homologación de determinados componentes o grupos de componentes de un tacógrafo, facilitará a las autoridades de homologación los demás componentes, ya homologados, así como las demás piezas necesarias para la construcción del tacógrafo completo, de manera que dichas autoridades puedan llevar a cabo los ensayos necesarios.

Articulo 5

Modificación de las homologaciones

1. El fabricante o su mandatario informarán sin demora a las autoridades de homologación que concedieron la homologación original acerca de cualquier cambio que se introduzca en el *software* o el *hardware* del tacógrafo o en la naturaleza de los materiales empleados en su fabricación que figuran en el expediente de homologación y presentarán una solicitud de modificación de la homologación.

2. Las autoridades de homologación podrán revisar o extender una homologación existente, o expedir una nueva, en función de la naturaleza y de las características de las modificaciones.

Se procederá a una «revisión» cuando la autoridad de homologación considere que las modificaciones en el *software* o el *hardware* del tacógrafo o en la naturaleza de los materiales empleados en su fabricación son de poca importancia. En estos casos, la autoridad de homologación expedirá los documentos revisados del expediente de homologación, indicando la naturaleza de las modificaciones efectuadas y la fecha de su aprobación. Bastará para satisfacer este requisito una versión actualizada del expediente de homologación en forma consolidada, acompañada de una descripción pormenorizada de las modificaciones.

Se procederá a una «extensión» cuando la autoridad de homologación considere que las modificaciones en el *software* o el *hardware* del tacógrafo o en la naturaleza de los materiales empleados en su fabricación son sustanciales. En estos casos, podrá solicitar que se lleven a cabo nuevos ensayos, de lo cual informará al fabricante o a su mandatario. Si estos ensayos resultan satisfactorios, la autoridad de homologación expedirá un certificado de homologación revisado que contendrá un número que remitirá a la extensión concedida. El certificado de homologación mencionará el motivo de la extensión y la fecha de expedición.

3. El índice del expediente de homologación indicará la fecha de la extensión o revisión más reciente de la homologación, o la fecha de la consolidación más reciente de la versión actualizada de la homologación.

4. Será necesaria una nueva homologación cuando las modificaciones solicitadas del tacógrafo homologado o de sus componentes obligarían a expedir un nuevo certificado de seguridad o de interoperabilidad.

Articulo 6

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Será aplicable a partir del 2 de marzo de 2016.

Sin embargo, los anexos serán aplicables a partir del 2 de marzo de 2019, a excepción del apéndice 16, que será aplicable a partir del 2 de marzo de 2016.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 18 de marzo de 2016.

Por la Comisión

El Presidente

Jean-Claude JUNCKER

ANEXO I C

Condiciones de fabricación, ensayo, instalación y control

INTRODUCCIÓN

El sistema de tacógrafo digital de primera generación está desplegado desde el 1 de mayo de 2006. Podrá utilizarse hasta el final de su vida útil para el transporte nacional. En el caso del transporte internacional, sin embargo, 15 años después de la entrada en vigor del presente Reglamento de la Comisión todos los vehículos deberán estar equipados con el tacógrafo inteligente de segunda generación conforme que introduce el presente Reglamento.

El presente anexo contiene las condiciones relativas a la segunda generación de aparatos de control y tarjetas de tacógrafo. A partir de su fecha de introducción, se instalará el aparato de control de segunda generación en los vehículos matriculados por vez primera, y se expedirán tarjetas de tacógrafo de segunda generación.

Con el fin de fomentar una integración gradual del sistema de tacógrafo de segunda generación,

— las tarjetas de tacógrafo de segunda generación se diseñarán para ser también utilizadas en las unidades instaladas en vehículos de primera generación,

— no se exigirá la sustitución de las tarjetas de tacógrafo de primera generación válidas en la fecha de introducción.

Esto permitirá a los conductores conservar una única tarjeta de conductor y utilizar ambos sistemas con ella.

Los aparatos de control de segunda generación, sin embargo, solo se calibrarán utilizando tarjetas de taller de segunda generación.

El presente anexo contiene todos los requisitos relacionados con la interoperabilidad entre la primera y la segunda generación del sistema de tacógrafo.

El apéndice 15 contiene más detalles sobre cómo gestionar la coexistencia de los dos sistemas.

Lista de apéndices

1 DEFINICIONES

A los efectos del presente anexo, se aplicarán las siguientes definiciones:

a) Activación:

Fase en que el tacógrafo pasa a ser totalmente operativo y realiza todas sus funciones, incluidas las de seguridad, mediante el uso de una tarjeta de taller.

b) Autenticación:

Función con la que se establece y verifica una identidad.

c) Autenticidad:

Propiedad de que una información proceda de alguien cuya identidad pueda verificarse.

d) Autodiagnóstico (BIT):

Ensayo que se lleva a cabo a petición del operario o por orden de un equipo externo.

e) Día civil:

Día comprendido entre las 00.00 y las 24.00 horas. Todos los días se referirán al tiempo universal coordinado (UTC).

f) Calibrado (de un tacógrafo digital inteligente):

Actualización o confirmación de los parámetros del vehículo que han de guardarse en la memoria de datos. Los parámetros del vehículo incluyen la identificación del vehículo (VIN, VRN y el Estado miembro donde se matriculó el vehículo) y las características del vehículo (w, k, l, tamaño de los neumáticos, valor de ajuste del dispositivo limitador de la velocidad, en su caso, hora UTC actual, lectura actual del cuentakilómetros); durante el calibrado de un aparato de control, los tipos y los identificadores de todos los precintos pertinentes de la homologación también se almacenarán en la memoria de datos.

Toda actualización o confirmación únicamente de la hora UTC se considerará un ajuste de la hora y no un calibrado, siempre que no contravenga el requisito 409.

Para calibrar un aparato de control se precisa una tarjeta de taller.

g) Número de tarjeta:

Secuencia de 16 caracteres alfanuméricos que identifica una tarjeta de tacógrafo en un Estado miembro. El número de tarjeta incluye un índice consecutivo de la tarjeta (en su caso), un índice de sustitución de la tarjeta y un índice de renovación de la tarjeta.

Por consiguiente, cada tarjeta se identifica de manera única con el código del Estado miembro que la expide y con el número de la propia tarjeta.

h) Índice consecutivo de la tarjeta:

Decimocuarto carácter alfanumérico del número de la tarjeta. Este carácter sirve para diferenciar las distintas tarjetas asignadas a una empresa, a un taller o a una autoridad de control con derecho a utilizar varias tarjetas de tacógrafo. La empresa, el taller o la autoridad de control se identifican con los trece primeros caracteres del número de la tarjeta.

i) Índice de renovación de la tarjeta:

Decimosexto carácter alfanumérico del número de la tarjeta. Este carácter se incrementa en una unidad cada vez que se renueva la tarjeta de tacógrafo.

j) Índice de sustitución de la tarjeta:

Decimoquinto carácter alfanumérico del número de la tarjeta. Este carácter se incrementa en una unidad cada vez que se sustituye la tarjeta de tacógrafo.

k) Coeficiente característico del vehículo:

Característica numérica que da el valor de la señal de salida emitida por la pieza prevista en el vehículo para su conexión con el aparato de control (toma de salida de la caja de cambio en algunos casos, rueda del vehículo en otros casos), cuando el vehículo recorre la distancia de un kilómetro, medida en condiciones normales de ensayo, según se definen en el requisito 414. El coeficiente característico se expresa en impulsos por kilómetro (w = … imp/km).

l) Tarjeta de empresa:

Tarjeta de tacógrafo expedida por las autoridades de un Estado miembro a favor de una empresa de transporte que necesita utilizar vehículos equipados de tacógrafo, que identifica a dicha empresa de transporte y permite visualizar, transferir e imprimir los datos almacenados en los tacógrafos y bloqueados por tal empresa.

m) Constante del aparato de control:

Característica numérica que da el valor de la señal de entrada necesaria para obtener la indicación y el registro de una distancia recorrida de un kilómetro; dicha constante deberá expresarse en impulsos por kilómetro (k = … imp/km).

n) Tiempo de conducción continua (contabilizado por el aparato de control) ([1]):

El tiempo de conducción continua se calcula a partir de los tiempos de conducción acumulados actuales de un conductor en particular, contados desde el momento en que termina su último período de DISPONIBILIDAD o PAUSA/DESCANSO o INDETERMINADO ([2]) de 45 minutos o más [este período puede haberse dividido con arreglo al Reglamento (CE) n.º 561/2006 del Parlamento Europeo y del Consejo ([3])]. Los cálculos tienen en cuenta, según proceda, las actividades anteriores que han quedado registradas en la tarjeta de conductor. Si el conductor no ha insertado su tarjeta, los cálculos se basan en los registros de la memoria de datos correspondientes al período actual en que no hubo tarjeta insertada y a la ranura que corresponda.

o) Tarjeta de control:

Tarjeta de tacógrafo expedida por las autoridades de un Estado miembro a una autoridad nacional de control competente, que identifica a este organismo y, de manera opcional, también al controlador, y que permite acceder a la información almacenada en la memoria de datos o en las tarjetas de conductor y, de manera opcional, en las tarjetas de taller con fines de lectura, impresión y/o transferencia de datos.

Asimismo, dará acceso a la función de control de calibrado en la carretera y a los datos contenidos en el lector de comunicaciones de teledetección temprana.

p) Tiempo de descanso acumulado (contabilizado por el aparato de control) ([1]):

El tiempo de descanso de la conducción acumulado, referido a un conductor en particular, se calcula a partir de los períodos acumulados actuales de DISPONIBILIDAD, PAUSA/DESCANSO o INDETERMINADOS ([2]) de 15 minutos o más, contados desde el momento en que terminara su último período de DISPONIBILIDAD o PAUSA/DESCANSO o INDETERMINADO ([2]) de 45 minutos o más [este período puede haberse dividido con arreglo al Reglamento (CE) n.º 561/2006].

Los cálculos tienen en cuenta, según proceda, las actividades anteriores que han quedado registradas en la tarjeta de conductor. Los cálculos no incluyen los períodos indeterminados que tengan una duración negativa (comienzo del período indeterminado > final del período indeterminado) a consecuencia de un solapamiento temporal entre dos aparatos de control distintos.

Si el conductor no ha insertado su tarjeta, los cálculos se basan en los registros de la memoria de datos correspondientes al período actual en que no hubo tarjeta insertada y a la ranura que corresponda.

([1]) Este modo de calcular el tiempo de conducción continua y el tiempo de descanso acumulado permite al aparato de control calcular el momento de activación del aviso de tiempo de conducción continua y no prejuzga la interpretación legal que deba hacerse de estos tiempos. Podrán utilizarse métodos alternativos para calcular el tiempo de conducción continua y el tiempo de descanso acumulado a fin de reemplazar estas definiciones si quedan obsoletas a raíz de las actualizaciones introducidas en otra legislación pertinente.

([2]) Los períodos INDETERMINADOS son aquellos en que la tarjeta de conductor no está insertada en el aparato de control y tampoco se introducen manualmente las actividades del conductor.

([3]) Reglamento (CE) n.º 561/2006 del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, relativo a la armonización de determinadas disposiciones en materia social en el sector de los transportes por carretera y por el que se modifican los Reglamentos (CEE) n.º 3821/85 y (CE) n.º 2135/98 del Consejo y se deroga el Reglamento (CEE) n.º 3820/85 del Consejo (DO L 102 de 11.4.2006, p. 1).

q) Memoria de datos:

Dispositivo de almacenamiento electrónico incorporado en el aparato de control.

r) Firma digital:

Datos adjuntos a un bloque de datos, o una transformación criptográfica de ellos, que permiten al destinatario comprobar la autenticidad e integridad de dicho bloque.

s) Transferencia:

Copia, junto con la firma digital, de una parte o de la totalidad de un conjunto de ficheros de datos almacenados en la memoria de datos de la unidad instalada en el vehículo o en la memoria de una tarjeta de tacógrafo, siempre que este proceso no altere ni suprima ninguno de los datos almacenados.

Los fabricantes de tacógrafos inteligentes instalados en el vehículo y los fabricantes de aparatos diseñados y concebidos para transferir ficheros de datos adoptarán todas las medidas necesarias para garantizar que los conductores o las empresas de transporte puedan transferir dichos datos en el menor tiempo posible.

La transferencia del fichero completo de datos sobre la velocidad del vehículo puede no ser necesaria para determinar el cumplimiento del Reglamento (CE) n.º 561/2006, aunque sí podrá utilizarse para otros fines, tales como la investigación de accidentes.

t) Tarjeta de conductor:

Tarjeta de tacógrafo expedida por las autoridades de un Estado miembro a un conductor concreto, que identifica a este último y permite almacenar los datos de su actividad.

u) Circunferencia efectiva de las ruedas:

Media de las distancias recorridas por cada una de las ruedas que arrastran el vehículo (ruedas motrices) al realizar una rotación completa. La medida de dichas distancias se efectuará en condiciones normales de ensayo, según se define en el requisito 414, y se expresará en la forma «l = … mm». Los fabricantes de los vehículos podrán sustituir la medición de estas distancias por un cálculo teórico que tenga en cuenta el reparto del peso sobre los ejes, con el vehículo descargado y en condiciones normales de marcha ([1]). Los métodos de dicho cálculo teórico deberán ser aprobados por la autoridad competente del Estado miembro y solo podrán tener lugar antes de la activación del tacógrafo.

v) Incidente:

Operación anormal detectada por el tacógrafo inteligente que puede deberse a un intento de fraude.

w) Dispositivo GNSS externo:

Instalación que contiene el receptor GNSS cuando la unidad instalada en el vehículo no es un módulo único, así como otros componentes necesarios para proteger la comunicación de los datos de posición al resto de la unidad instalada en el vehículo.

x) Fallo:

Operación anormal detectada por el tacógrafo inteligente y que puede deberse a un fallo de funcionamiento.

y) Receptor GNSS:

Dispositivo electrónico que recibe y procesa digitalmente las señales digitales de uno o más sistemas mundiales de navegación por satélite (GNSS por sus siglas en inglés) con el fin de proporcionar información de posición, velocidad y hora.

z) Instalación:

Montaje de un tacógrafo en un vehículo.

([1]) Reglamento (UE) n.º 1230/2012 de la Comisión, de 12 de diciembre de 2012, por el que se desarrolla el Reglamento (CE) n.º 661/2009 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos de homologación de tipo relativos a las masas y dimensiones de los vehículos de motor y de sus remolques y por el que se modifica la Directiva 2007/46/CE del Parlamento Europeo y del Consejo (DO L 353 de 21.12.2012, p. 31), en su versión modificada en último lugar.

aa) Interoperabilidad:

Capacidad de los sistemas y de los procesos subyacentes para intercambiar datos y compartir información.

bb) Interfaz:

Dispositivo entre sistemas que facilita los medios de comunicación a través de los cuales pueden conectarse y actuar entre sí.

cc) Posición:

Coordenadas geográficas del vehículo en un momento dado.

dd) Sensor de movimiento:

Parte del tacógrafo que ofrece una señal representativa de la velocidad del vehículo y/o de la distancia recorrida.

ee) Tarjeta no válida:

Tarjeta en la que se ha detectado un defecto, o que no ha superado la autenticación inicial, o que no ha alcanzado todavía la fecha de comienzo de validez, o que ha sobrepasado ya la fecha de expiración.

ff) Norma abierta:

Norma que figura en un documento de especificación de normas que está disponible sin contrapartida financiera o por una contrapartida simbólica, que cualquier persona puede copiar, distribuir o utilizar gratuitamente o por un precio simbólico.

gg) Fuera de ámbito:

Cuando el uso del aparato de control no es obligatorio, de conformidad con lo dispuesto en el Reglamento (CE) n.º 561/2006.

hh) Exceso de velocidad:

Rebasamiento de la velocidad autorizada para el vehículo, definido como un período de más de sesenta segundos durante el cual la velocidad medida del vehículo sobrepasa el valor de ajuste del dispositivo limitador de la velocidad, regulado con arreglo a la Directiva 92/6/CEE del Consejo ([1]), en su versión modificada en último lugar.

ii) Control periódico:

Conjunto de operaciones con las que se comprueba que el tacógrafo funciona correctamente, que sus valores de ajuste corresponden a los parámetros del vehículo y que no hay dispositivos de manipulación integrados en el tacógrafo.

jj) Impresora:

Componente del aparato de control que permite imprimir los datos almacenados.

kk) Comunicación de teledetección temprana:

Comunicación entre el dispositivo de comunicación de teledetección temprana y el lector de comunicación de teledetección temprana durante los controles de carretera selectivos encaminados a detectar una posible manipulación o utilización indebida del aparato de control.

ll) Dispositivo de comunicación a distancia:

Equipo de la unidad instalada en el vehículo que se utiliza para realizar controles de carretera selectivos.

([1]) Directiva 92/6/CEE del Consejo, de 10 de febrero de 1992, relativa a la instalación y a la utilización de dispositivos de limitación de velocidad en determinadas categorías de vehículos de motor en la Comunidad (DO L 57 de 2.3.1992, p. 27).

mm) Lector de comunicación de teledetección temprana:

El sistema utilizado por los controladores para los controles de carretera selectivos.

nn) Renovación:

Asignación de una nueva tarjeta de tacógrafo cuando la tarjeta existente alcanza su fecha de expiración o se ha devuelto a la autoridad emisora por un fallo de funcionamiento. La renovación implica siempre la certeza de que no coexistirán dos tarjetas válidas.

oo) Reparación:

Cualquier reparación de un sensor de movimiento o de una unidad instalada en el vehículo o de un cable que requiera la desconexión de su fuente de alimentación, o su desconexión de otros componentes del tacógrafo, o la apertura del sensor de movimiento o de la unidad instalada en el vehículo.

pp) Sustitución de la tarjeta:

Emisión de una tarjeta de tacógrafo en sustitución de una tarjeta existente que se haya declarado perdida, robada o defectuosa y que no se haya devuelto a la autoridad expedidora. La sustitución implica siempre el riesgo de que coexistan dos tarjetas válidas.

qq) Certificación de seguridad:

Procedimiento por el que un organismo de certificación de Criterios Comunes garantiza que el aparato de control (o componente) o la tarjeta de tacógrafo que se investiga cumple los requisitos de seguridad definidos en los correspondientes perfiles de protección.

rr) Comprobación automática:

Comprobaciones que realiza de manera cíclica y automática el aparato de control para detectar posibles fallos.

ss) Medición de la hora:

Registro digital permanente de la fecha y la hora del tiempo universal coordinado (UTC).

tt) Ajuste de la hora:

Ajuste automático de la hora actual a intervalos regulares y con un máximo de tolerancia de un minuto, o un ajuste efectuado durante el calibrado.

uu) Tamaño de los neumáticos:

Designación de las dimensiones de los neumáticos (ruedas motrices externas) con arreglo a la Directiva 92/23/CEE del Consejo ([1]), en su versión modificada en último lugar.

vv) Identificación del vehículo:

Números que identifican el vehículo: número de matrícula (VRN), con indicación del Estado miembro donde está matriculado, y número de identificación (VIN) ([2]).

ww) Semana (a efectos de cálculo en el aparato de control):

Período que va de las 00.00 horas de un lunes a las 24.00 horas de un domingo, referido al tiempo universal coordinado.

([1]) Directiva 92/23/CEE del Consejo, de 31 de marzo de 1992, sobre los neumáticos de los vehículos de motor y de sus remolques así como de su montaje (DO L 129 de 14.5.1992, p. 95).

([2]) Directiva 76/114/CEE del Consejo, de 18 de diciembre de 1975, relativa a la aproximación de las legislaciones de los Estados Miembros sobre las placas e inscripciones reglamentarias, así como a su emplazamiento y modo de colocación, en lo que se refiere a los vehículos a motor y a sus remolques (DO L 24 de 30.1.1976, p. 1).

xx) Tarjeta de taller:

Tarjeta de tacógrafo expedida por las autoridades de un Estado miembro a personal designado de un fabricante o instalador de tacógrafos, fabricante de vehículos o taller aprobado por dicho Estado miembro, que identifica a su titular y le permite el ensayo, calibrado y activación de tacógrafos y/o la transferencia de datos de estos.

yy) Adaptador:

Dispositivo que proporciona una señal en todo momento representativa de la velocidad del vehículo o la distancia recorrida, excepto el utilizado para la detección de movimiento independiente, y que:

— se instala y utiliza exclusivamente en vehículos de las categorías M1 y N1 (según se definen en el anexo II de la Directiva 2007/46/CEE del Parlamento Europeo y del Consejo ([1]), en su versión modificada más reciente) puestos en servicio a partir del 1 de mayo de 2006;

— se instala cuando mecánicamente resulta imposible instalar ningún otro tipo de sensor de movimiento existente que por su parte cumpla las disposiciones de este anexo y sus apéndices 1 a 15;

— se instala entre la unidad instalada en el vehículo y el lugar en el que se generan los impulsos de velocidad o distancia mediante sensores integrados o interfaces alternativas;

— desde la perspectiva de la unidad instalada en el vehículo, el comportamiento del adaptador es el mismo que se obtendría conectando a la unidad instalada en el vehículo un sensor de movimiento conforme a las disposiciones del presente anexo y sus apéndices 1 a 16.

El uso de este tipo de adaptador en los vehículos indicados anteriormente permitirá la instalación y la utilización correcta de una unidad instalada en el vehículo conforme a todos los requisitos del presente anexo.

En lo que respecta a esos vehículos, el tacógrafo inteligente incluye los cables, un adaptador y una unidad instalada en el vehículo.

zz) Integridad de los datos:

Exactitud y coherencia de los datos almacenados, indicada por la ausencia de alteración de los datos entre dos actualizaciones de un registro de datos. La integridad implica que los datos son copia exacta de la versión original, por ejemplo, que no han sido corrompidos en el proceso de su escritura o lectura en una tarjeta de tacógrafo o un equipo dedicado o durante la transmisión a través de un canal de comunicaciones.

aaa) Privacidad de los datos:

Conjunto de las medidas técnicas adoptadas para garantizar la adecuada aplicación de los principios establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo ([2]), así como de los establecidos en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([3]).

bbb) Sistema de tacógrafo inteligente:

Los aparatos de control, las tarjetas de tacógrafo y el conjunto de todos los equipos que interactúan, directa o indirectamente, durante su fabricación, instalación, utilización, ensayo y control, como las tarjetas, el lector de comunicación a distancia y cualquier otro equipo utilizado para transferencia de datos, análisis de datos, calibrado, generación, gestión o introducción de elementos de seguridad, etc.

ccc) Fecha de introducción:

Treinta y seis meses después de la entrada en vigor de las disposiciones específicas indicadas en el artículo 11 del Reglamento (UE) n.º 165/2014 del Parlamento Europeo y del Consejo ([4]).

([1]) Directtiva 2007/46/CE del Parlamento Europeo y del Consejo, de 5 de septiembre de 2007, por la que se crea un marco para la homologación de los vehículos de motor y de los remolques, sistemas, componentes y unidades técnicas independientes destinados a dichos vehículos (Directiva marco) (DO L 263 de 9.10.2007, p. 1).

([2]) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31)

([3]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

([4]) Reglamento (UE) n.º 165/2014 del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, relativo a los tacógrafos en el transporte por carretera, por el que se deroga el Reglamento (CEE) n.º 3821/85 del Consejo relativo al aparato de control en el sector de los transportes por carretera y se modifica el Reglamento (CE) n.º 561/2006 del Parlamento Europeo y del Consejo relativo a la armonización de determinadas disposiciones en materia social en el sector de los transportes por carretera (DO L 60 de 28.2.2014, p. 1).

Esta es la fecha a partir de la cual los vehículos matriculados por primera vez:

— *estarán dotados de un tacógrafo conectado a un servicio de posicionamiento basado en un sistema de navegación por satélite;*

— *podrán comunicar datos para controles de carretera selectivos a las autoridades de control competentes mientras el vehículo está en movimiento;*

— *y podrán ir equipados de interfaces normalizadas que permitan que un dispositivo externo utilice en modo operativo los datos registrados o producidos por el tacógrafo*.

ddd) Perfil de protección:

Documento utilizado como parte del proceso de certificación según Criterios Comunes, que facilita una especificación independiente de la implementación de los requisitos de seguridad de aseguramiento de la información.

eee) Exactitud del GNSS:

En el contexto del registro de la posición a partir del sistema mundial de navegación por satélite (GNSS) con tacógrafos, el valor de la dilución horizontal de la precisión (HDOP), calculado como el mínimo de los valores de HDOP recogidos en los sistemas GNSS disponibles.

2 CARACTERÍSTICAS GENERALES Y FUNCIONES DEL APARATO DE CONTROL

2.1 **Características generales**

El aparato de control sirve para registrar, almacenar, visualizar, imprimir y enviar datos relacionados con las actividades del conductor.

Todo vehículo que lleve instalado un aparato de control conforme a lo dispuesto en el presente anexo debe incorporar además un indicador de velocidad y un cuentakilómetros. Estas funciones pueden estar incluidas en el aparato de control.

01) El aparato de control incluye cables, un sensor de movimiento y una unidad instalada en el vehículo.

02) La interfaz entre los sensores de movimiento y las unidades instaladas en los vehículos deberá ajustarse a los requisitos especificados en el apéndice 11.

03) La unidad instalada en el vehículo deberá estar conectada a uno o más sistemas mundiales de navegación por satélite, tal como se especifica en el apéndice 12.

04) La unidad instalada en el vehículo deberá comunicar con los lectores de comunicación de teledetección temprana, tal como se especifica en el apéndice 14.

05) La unidad instalada en el vehículo podrá incluir una interfaz ITS, que se especifica en el apéndice 13.

El aparato de control podrá estar conectado a otros dispositivos mediante interfaces adicionales y/o a través de la interfaz ITS opcional.

06) Ninguna función o dispositivo, homologado o no, que se incluya o se conecte al aparato de control deberá interferir ni ser capaz de interferir con el funcionamiento correcto y seguro del aparato de control ni con lo dispuesto en el presente Reglamento.

Los usuarios del aparato de control se identifican ante el aparato a través de las tarjetas de tacógrafo.

07) El aparato de control proporciona derechos de acceso selectivo a los datos y funciones según el tipo o la identidad del usuario.

El aparato de control registra y almacena datos en su memoria, en el dispositivo de comunicación a distancia y en las tarjetas de tacógrafo.

Esto se efectúa con arreglo a la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ([1]), con la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas ([2]), y de conformidad con el artículo 7 del Reglamento (UE) n.º 165/2014.

2.2 **Funciones**

08) El aparato de control deberá garantizar las funciones siguientes:

— control de la inserción y extracción de las tarjetas,

— medición de la velocidad, distancia y posición,

— medición de la hora,

— supervisión de las actividades del conductor,

— supervisión del régimen de conducción,

— entradas manuales de los conductores:

  — entrada de los lugares donde comienzan o terminan los períodos de trabajo diarios,

  — entrada manual de las actividades del conductor,

  — entrada de condiciones específicas,

— gestión de los bloqueos introducidos por la empresa,

— supervisión de las actividades de control,

— detección de incidentes o fallos,

— autodiagnóstico y comprobaciones automáticas,

— lectura de los datos almacenados en la memoria,

— registro y almacenamiento de datos en la memoria,

— lectura de las tarjetas de tacógrafo,

— registro y almacenamiento de datos en las tarjetas de tacógrafo,

— visualización,

— impresión,

— advertencias,

— transferencia de datos a medios externos,

— comunicación a distancia para controles de carretera selectivos,

— envío de datos a dispositivos adicionales,

— calibrado,

— control del calibrado en carretera,

— ajuste de la hora.

([1]) DO L 281 de 23.11.1995, p. 31.
([2]) DO L 201 de 31.7.2002, p. 37.

2.3 **Modos de funcionamiento**

09) El aparato de control deberá tener cuatro modos de funcionamiento:

— modo operativo,

— modo de control,

— modo de calibrado,

— modo de empresa.

10) El aparato de control pasará al siguiente modo de funcionamiento según las tarjetas de tacógrafo válidas que se inserten en los dispositivos de interfaz: A efectos de determinar el modo de funcionamiento, es irrelevante la generación de la tarjeta de tacógrafo, siempre que la tarjeta insertada sea válida. Una tarjeta de taller de primera generación se considerará siempre no válida cuando se inserte en una unidad instalada en el vehículo de segunda generación.

Modo de funcionamiento		Ranura del conductor				
		Sin tarjeta	Tarjeta de conductor	Tarjeta de control	Tarjeta de taller	Tarjeta de empresa
Ranura del segundo conductor	Sin tarjeta	operativo	operativo	de control	de calibrado	de empresa
	Tarjeta de conductor	operativo	operativo	de control	de calibrado	de empresa
	Tarjeta de control	de control	de control	de control (*)	operativo	operativo
	Tarjeta de taller	de calibrado	de calibrado	operativo	de calibrado (*)	operativo
	Tarjeta de empresa	de empresa	de empresa	operativo	operativo	de empresa (*)

(*) En estas situaciones, el aparato de control utilizará exclusivamente la tarjeta de tacógrafo insertada en la ranura del conductor.

11) El aparato de control no tendrá en cuenta las tarjetas no válidas que se inserten, excepto si se visualizan, imprimen o transfieren los datos almacenados en una tarjeta que ha expirado, cosa que deberá ser posible.

12) Todas las funciones enumeradas en el apartado 2.2 estarán disponibles en cualquier modo de funcionamiento, con las siguientes excepciones:

— la función de calibrado solo está disponible en el modo de calibrado,

— la función de control del calibrado en carretera solo está disponible en el modo de control,

— la función de gestión de los bloqueos introducidos por la empresa solo está disponible en el modo de empresa,

— la función de supervisión de las actividades de control solo funciona en el modo de control,

— la función de transferencia no está disponible en el modo operativo (salvo en el caso indicado en el requisito 193), exceptuada la descarga de datos de una tarjeta de conductor si no hay otro tipo de tarjeta insertada en la VU.

13) El aparato de control podrá enviar cualquier dato a la pantalla, a la impresora o a interfaces externas, con las siguientes excepciones:

— en el modo operativo, toda identificación personal (nombre y apellidos) que no corresponda a una tarjeta de tacógrafo insertada se borrará por completo, y todo número de tarjeta que no corresponda a una tarjeta de tacógrafo insertada se borrará parcialmente (se borrarán los caracteres impares, de izquierda a derecha);

— en el modo de empresa, los datos relativos al conductor (requisitos 102, 105 y 108) tan solo podrán enviarse a dispositivos externos durante los períodos exentos de bloqueo o que no haya bloqueado otra empresa (identificada por los 13 primeros dígitos del número de la tarjeta de empresa);

— si no se ha insertado ninguna tarjeta en el aparato de control, solo podrán enviarse los datos relativos al conductor que correspondan al día actual y a los ocho días civiles anteriores;

— los datos personales procedentes de la VU no podrán enviarse a través de la interfaz ITS de la VU a menos que se haya verificado el consentimiento del conductor al que se refieran los datos;

— el período de validez operativa normal de las unidades instaladas en vehículos es de quince años a partir de la fecha de expedición de los certificados de dichas unidades, pero podrán utilizarse durante tres meses adicionales solo para la transferencia de datos.

2.4 **Seguridad**

La seguridad del sistema tiene por objeto proteger la memoria de datos, de manera que se evite el acceso a la misma de terceros no autorizados, se excluya la manipulación de información y se detecte cualquier tentativa en ese sentido; así se protege la integridad y autenticidad de los datos intercambiados entre el sensor de movimiento y la unidad instalada en el vehículo, de los datos intercambiados entre el aparato de control y las tarjetas de tacógrafo y de los datos intercambiados entre el aparato de control y el dispositivo GNSS externo, se protege la confidencialidad, integridad y autenticidad de los datos intercambiados a través de la comunicación de teledetección temprana con fines de control y se verifica la integridad y autenticidad de los datos transferidos.

14) Al objeto de lograr la seguridad del sistema, los siguientes componentes deberán cumplir los requisitos de seguridad que se definen en sus perfiles de protección, según exige el apéndice 10:

— unidad instalada en el vehículo,

— tarjeta de tacógrafo,

— sensor de movimiento,

— dispositivo GNSS externo (este perfil solo es necesario y aplicable para la variante del GNSS externo).

3 CONDICIONES DE FABRICACIÓN Y FUNCIONAMIENTO DEL APARATO DE CONTROL

3.1 **Control de la inserción y extracción de las tarjetas**

15) El aparato de control supervisará los dispositivos de interfaz para detectar la inserción y extracción de las tarjetas.

16) Nada más insertar la tarjeta, el aparato de control detectará si se trata de una tarjeta de tacógrafo válida y, en tal caso, identificará el tipo y la generación de la tarjeta.

Si en el aparato de control se ha insertado ya una tarjeta con el mismo número de tarjeta y un índice de renovación superior, la tarjeta será declarada no válida.

Si en el aparato de control se ha insertado ya una tarjeta con los mismos número de tarjeta y de índice de renovación, pero con un índice de sustitución superior, la tarjeta será declarada no válida.

17) Las tarjetas de tacógrafo de primera generación serán consideradas no válidas por el aparato de control una vez que la posibilidad de utilizar tarjetas de tacógrafo de primera generación haya sido suprimida por un taller, de conformidad con el apéndice 15 (req. MIG003).

18) Las tarjetas de taller de primera generación que se inserten en aparatos de control de la segunda generación se considerarán no válidas.

19) El aparato de control deberá estar construido de tal modo que las tarjetas de tacógrafo queden fijas en su posición al insertarlas correctamente en los dispositivos de interfaz.

20) La extracción de las tarjetas de tacógrafo solo deberá ser posible con el vehículo parado y después de haberse almacenado en dichas tarjetas los datos pertinentes. La extracción de la tarjeta exigirá la intervención directa del usuario.

3.2 **Medición de la velocidad, la posición y la distancia**

21) El sensor de movimiento (en su caso, integrado en el adaptador) es la fuente principal para la medición de la velocidad y la distancia.

22) Esta función medirá de forma continua y permitirá indicar en el cuentakilómetros el valor correspondiente a la distancia total recorrida por el vehículo utilizando los impulsos proporcionados por el sensor de movimiento.

23) Esta función medirá de forma continua y permitirá indicar la velocidad del vehículo utilizando los impulsos proporcionados por el sensor de movimiento.

24) Asimismo, la función de medición de la velocidad indicará si el vehículo está en movimiento o parado. Se considerará que el vehículo está en movimiento en cuanto la función, a través del sensor de movimiento, detecte más de 1 imp/seg durante al menos cinco segundos. De lo contrario, se considerará que el vehículo está parado.

25) Los dispositivos indicadores de la velocidad (velocímetro) y de la distancia total recorrida (cuentakilómetros) instalados en un vehículo que incorpore un aparato de control conforme a lo dispuesto en el presente Reglamento deberán cumplir las condiciones relativas a las tolerancias máximas (véanse los puntos 3.2.1 y 3.2.2) establecidas en el presente anexo.

26) Para detectar cualquier manipulación de los datos de movimiento, la información importada del sensor de movimiento deberá ser confirmada por aquella otra relativa al movimiento del vehículo procedente del receptor GNSS y, opcionalmente, de otra(s) fuente(s) independiente(s) del sensor de movimiento.

27) Esta función medirá la posición del vehículo a fin de permitir el registro automático de:

— las posiciones en que el conductor y/o el segundo conductor empiezan su período de trabajo diario;

— las posiciones en que el tiempo de conducción continua del conductor llega a un múltiplo de tres horas;

— las posiciones en que el conductor y/o el segundo conductor finalizan su período de trabajo diario.

3.2.1 *Medición de la distancia recorrida*

28) La distancia recorrida podrá medirse:

— bien de forma que se incluyan los movimientos en marcha adelante y en marcha atrás,

— bien únicamente en marcha adelante.

29) El aparato de control deberá medir la distancia entre 0 y 9 999 999,9 km.

30) La distancia medida estará comprendida en los siguientes límites de tolerancia (distancias de al menos 1 000 m):

— ± 1 % antes de la instalación,

— ± 2 % después de la instalación y de un control periódico,

— ± 4 % durante el uso.

31) La distancia medida tendrá una resolución igual o mejor que 0,1 km.

3.2.2 *Medición de la velocidad*

32) El aparato de control deberá medir la velocidad entre 0 y 220 km/h.

33) A fin de garantizar una tolerancia máxima de ± 6 km/h para la indicación de la velocidad durante el uso, y teniendo en cuenta:

— una tolerancia de ± 2 km/h para posibles variaciones de los valores de entrada (variaciones de los neumáticos, …),

— una tolerancia de ± 1 km/h en las mediciones realizadas durante la instalación o en los controles periódicos,

el aparato de control deberá medir la velocidad con una tolerancia de ± 1 km/h (a velocidad constante) para velocidades entre 20 y 180 km/h y para coeficientes característicos del vehículo entre 4 000 y 25 000 imp/km.

Nota: La resolución del almacenamiento de datos aporta una tolerancia adicional de ± 0,5 km/h a la velocidad registrada por el aparato de control.

34) La velocidad deberá medirse correctamente dentro de las tolerancias normales y antes de que hayan transcurrido dos segundos tras haberse producido un cambio de velocidad, si dicho cambio no sobrepasa una aceleración de 2 m/s^2.

35) La medición de la velocidad tendrá una resolución igual o mejor que 1 km/h.

3.2.3 *Medición de la posición*

36) El aparato de control medirá la posición absoluta del vehículo utilizando el receptor GNSS.

37) La posición absoluta se mide en coordenadas geográficas de latitud y longitud, en grados y minutos, con una resolución de 1/10 de minuto.

3.3 **Medición de la hora**

38) La función de medición de la hora deberá medir de forma continua y expresar digitalmente la fecha y la hora correspondientes al tiempo universal coordinado (UTC).

39) La fecha y la hora UTC deberán utilizarse para fechar los datos internos del aparato de control (registros, intercambio de datos) y para toda impresión especificada en el apéndice 4: «Documentos de impresión».

40) A fin de visualizar la hora local, existirá la posibilidad de cambiar el desfase horario que aparece en pantalla, en fracciones de media hora. Tan solo se podrá compensar dicho desfase añadiendo múltiplos negativos o positivos de fracciones de media hora.

41) La desviación de la hora no superará los ± 2 segundos por día en condiciones de homologación, en ausencia de ajustes de la hora.

42) La hora medida tendrá una resolución igual o superior a un segundo.

43) En las condiciones de homologación, la medición de la hora no deberá verse afectada por interrupciones del suministro eléctrico de duración inferior a doce meses.

3.4 **Supervisión de las actividades del conductor**

44) Esta función deberá controlar permanentemente y por separado las actividades de un conductor y un segundo conductor.

45) Las actividades del conductor pueden ser CONDUCCIÓN, TRABAJO, DISPONIBILIDAD o PAUSA/DESCANSO.

46) El conductor o el segundo conductor deberán tener la posibilidad de seleccionar manualmente las actividades de TRABAJO, DISPONIBILIDAD o PAUSA/DESCANSO.

47) Cuando el vehículo esté en movimiento, el aparato seleccionará automáticamente la actividad de CONDUCCIÓN para el conductor y la actividad de DISPONIBILIDAD para el segundo conductor.

48) Cuando el vehículo se detenga, se seleccionará automáticamente la actividad de TRABAJO para el conductor.

49) Si el primer cambio de actividad a DESCANSO o DISPONIBILIDAD tiene lugar antes de que hayan transcurrido 120 segundos tras haber cambiado automáticamente a TRABAJO por haberse detenido el vehículo, se entenderá que ha tenido lugar a la hora en que se detuvo el vehículo (por consiguiente, podría cancelar el cambio a TRABAJO).

50) Esta función deberá notificar los cambios de actividad a las funciones de registro con una resolución de un minuto.

51) A partir de un minuto cualquiera, si se registra alguna actividad de CONDUCCIÓN en los minutos inmediatamente anterior y posterior, se considerará que todo el minuto es de actividad de CONDUCCIÓN.

52) Dado un minuto cualquiera que no se considere de CONDUCCIÓN con arreglo al requisito 051, se considerará que todo el minuto será de un mismo tipo de actividad, concretamente la que haya tenido lugar de forma continuada y durante más tiempo durante ese minuto (en caso de haber dos actividades de la misma duración, la que se haya producido en último lugar).

53) Esta función también deberá controlar permanentemente el tiempo de conducción continua y el tiempo de descanso acumulado del conductor.

3.5 **Supervisión del régimen de conducción**

54) Esta función deberá controlar permanentemente el régimen de conducción.

55) Si hay dos tarjetas de conductor insertadas en el aparato, habrá que seleccionar el régimen EN EQUIPO. De otro modo se seleccionará el régimen EN SOLITARIO.

3.6 **Entradas de los conductores**

3.6.1 *Introducción de los lugares donde comienzan o terminan los períodos de trabajo diarios*

56) Esta función deberá permitir la introducción de los lugares donde, según el conductor y/o el segundo conductor, comienzan o terminan sus períodos de trabajo diarios.

57) Se entiende por lugar el país y, cuando proceda, la región, que se introducirán o confirmarán manualmente.

58) En el momento de extraer la tarjeta del conductor, el aparato de control deberá pedir al conductor (o segundo conductor) que introduzca el «lugar donde termina el período de trabajo diario».

59) El conductor deberá introducir entonces el lugar en que se encuentra actualmente el vehículo, que se considerará una entrada temporal.

60) Se podrán introducir los lugares donde comiencen y/o terminen los períodos de trabajo diarios a través de comandos de los menús. Si se produce más de una entrada en un minuto cualquiera, tan solo quedarán registrados el último lugar de comienzo y el último lugar de finalización de trabajo introducidos en el marco temporal de dicho minuto.

3.6.2 *Introducción manual de las actividades del conductor y del consentimiento del conductor a la interfaz ITS*

61) El aparato de control permitirá la introducción manual de actividades única y exclusivamente al insertar la tarjeta de conductor (o de taller). Para la introducción manual de actividades, se utilizarán la fecha y hora locales de la zona horaria (desfase UTC) configuradas para la unidad instalada en el vehículo.

Al insertar la tarjeta de conductor o de taller, se recordarán al titular de la tarjeta:

— la fecha y la hora de la última extracción de la tarjeta;

— opcionalmente: el desfase horario local configurado para la unidad instalada en el vehículo.

Al insertar por primera vez determinada tarjeta de conductor o de taller desconocida en la unidad instalada en el vehículo, se invitará al titular de la tarjeta a dar su consentimiento a la salida de datos personales relacionados con el tacógrafo a través de la interfaz ITS opcional.

En cualquier momento, podrá habilitarse o inhabilitarse el consentimiento del conductor (respectivamente, del taller) a través de comandos del menú, siempre que esté insertada la tarjeta de conductor (respectivamente, de taller).

Se podrán introducir actividades observando las siguientes restricciones:

— el tipo de actividad podrá ser: TRABAJO, DISPONIBILIDAD o PAUSA/DESCANSO;

— la hora de comienzo y finalización de cada actividad estará enmarcada en el intervalo que transcurre entre la última extracción de la tarjeta y su inserción actual;

— no deberá producirse ningún solapamiento temporal entre las diversas actividades.

Si fuere necesario, podrán realizarse entradas manuales al insertar, por vez primera, una tarjeta de conductor (o de taller) no utilizada previamente.

El procedimiento de introducción manual de actividades incluirá tantas fases consecutivas como sea necesario para configurar los distintos tipos de actividad y la hora de comienzo y finalización de cada actividad. El titular de la tarjeta podrá optar por no declarar actividad alguna durante cualquier intervalo de tiempo entre la última extracción de la tarjeta y la inserción actual.

Durante el proceso de introducción manual de actividades asociado a la inserción de la tarjeta, y en los casos pertinentes, el titular de la tarjeta podrá introducir, asimismo:

— un lugar en que haya terminado un período de trabajo diario precedente, asociado a la hora pertinente (sobreescribiendo así la entrada realizada con motivo de la última extracción de la tarjeta), o

— un lugar en que comience el período de trabajo diario actual, asociado a la hora pertinente.

Si el titular de la tarjeta no introduce el lugar donde comienza o finaliza el período de trabajo durante el proceso de introducción manual asociado a la inserción de la tarjeta, se considerará que declara que su período de trabajo no ha cambiado desde la última extracción de la tarjeta. La próxima entrada de un lugar donde termina el período de trabajo diario precedente sobreescribirá, pues, la entrada temporal realizada en la última extracción de la tarjeta.

Si se introduce un lugar, este quedará registrado en la tarjeta de tacógrafo pertinente.

Se interrumpirán las introducciones manuales en los siguientes casos:

— cuando se extraiga la tarjeta, o

— cuando el vehículo se mueva permaneciendo insertada la tarjeta en la ranura del conductor.

Se permiten otras interrupciones como, por ejemplo, la desconexión tras un cierto período de inactividad del usuario. En caso de interrumpirse el proceso de introducción manual, el aparato de control validará cualquier entrada completa de lugar y actividad ya realizada (indicando de forma inequívoca el lugar y la hora, o el tipo de actividad y la hora de comienzo y finalización).

Si se inserta la tarjeta de un segundo conductor o de un taller mientras está en curso la introducción manual de actividades para una tarjeta previamente insertada, se permitirá completar dichas entradas correspondientes a la tarjeta anterior antes de dar paso a la introducción manual de entradas relativas a la segunda tarjeta.

El titular de la tarjeta podrá realizar entradas manualmente conforme al siguiente procedimiento mínimo:

— introducir manualmente y por orden cronológico las actividades realizadas durante el período comprendido entre la última extracción de la tarjeta y la actual inserción;

— la hora de comienzo de la primera actividad se ajustará a la hora de extracción de la tarjeta; la hora de comienzo de cada entrada sucesiva deberá ajustarse al momento inmediatamente posterior a la hora de finalización de la entrada precedente; deberá indicarse para cada actividad el tipo de actividad y la hora de finalización.

El procedimiento concluirá cuando la hora de finalización de una actividad introducida manualmente coincida con la hora de inserción de la tarjeta. A continuación, el aparato de control podrá permitir opcionalmente al titular de la tarjeta modificar las actividades introducidas manualmente, hasta validarlas seleccionando un comando específico. Una vez validadas las actividades, ya no se podrán realizar modificaciones.

3.6.3 *Entrada de condiciones específicas*

62) El aparato de control permitirá al conductor introducir, en tiempo real, las dos condiciones específicas siguientes:

— «FUERA DE ÁMBITO» (comienzo, final),

— «TRAYECTO EN TRANSBORDADOR/TREN» (comienzo, final).

La condición «TRAYECTO EN TRANSBORDADOR/TREN» no puede darse si está abierta la condición «FUERA DE ÁMBITO».

Si la condición «FUERA DE ÁMBITO» está abierta, el aparato de control tendrá que cerrarla inmediatamente en caso de insertarse o extraerse una tarjeta de conductor.

El hecho de estar abierta la condición «FUERA DE ÁMBITO» impedirá los siguientes incidentes y advertencias:

— conducción sin tarjeta adecuada,

— advertencias asociadas al tiempo de conducción continua.

El indicador de comienzo de «TRAYECTO EN TRANSBORDADOR/TREN» deberá activarse antes de apagar el motor en el transbordador/tren.

Un «TRAYECTO EN TRANSBORDADOR/TREN» abierto deberá cerrarse cuando se produzca alguna de las circunstancias siguientes:

— el conductor finaliza de forma manual el «TRAYECTO EN TRANSBORDADOR/TREN»,

— el conductor extrae su tarjeta.

Un «TRAYECTO EN TRANSBORDADOR/TREN» abierto se cerrará cuando deje de ser válido sobre la base de las normas establecidas en el Reglamento (CE) n.º 561/2006.

3.7 **Gestión de los bloqueos introducidos por la empresa**

63) Esta función deberá permitir la gestión de los bloqueos que haya introducido una empresa con el fin de restringir el acceso a sus propios datos en el modo de empresa.

64) Estos bloqueos consisten en una fecha/hora inicial (activación del bloqueo) y una fecha/hora final (desactivación del bloqueo) asociadas con la identificación de la empresa, indicada por el número de la tarjeta de la empresa (al activarse el bloqueo).

65) Los bloqueos se activan y desactivan siempre en tiempo real.

66) Sólo podrá desactivar el bloqueo la empresa que lo haya activado (identificada por los trece primeros dígitos del número de la tarjeta de la empresa), o bien

67) El bloqueo se desactivará automáticamente si otra empresa activa un bloqueo.

68) En los casos en los que la empresa que activa el bloqueo es la misma empresa que introdujo el anterior bloqueo, se considerará que el bloqueo previo no ha sido desactivado y se encuentra todavía activo.

3.8 **Supervisión de las actividades de control**

69) Esta función supervisa las actividades de VISUALIZACIÓN, IMPRESIÓN, TRANSFERENCIA de la VU y de la tarjeta y control del CALIBRADO EN CARRETERA que se lleven a cabo en el modo de control.

70) Esta función también supervisa las actividades de CONTROL DEL EXCESO DE VELOCIDAD en el modo de control. Se entenderá que se ha producido un control del exceso de velocidad cuando, estando en el modo de control, se haya enviado la señal de «exceso de velocidad» a la impresora o a la pantalla, o cuando la memoria de datos de la VU haya transferido datos sobre «incidentes y fallos».

3.9 **Detección de incidentes o fallos**

71) Esta función detecta los siguientes incidentes o fallos:

3.9.1 *Incidente «Inserción de una tarjeta no válida»*

72) Este incidente se produce al insertar una tarjeta no válida, al insertar una tarjeta de conductor ya sustituida y/o cuando expira una tarjeta válida insertada.

3.9.2 *Incidente «Conflicto de tarjetas»*

73) Este incidente se produce cuando se produce alguna de las combinaciones de tarjetas válidas señaladas con X en el siguiente cuadro:

Conflicto de tarjetas		Ranura del conductor				
		Sin tarjeta	Tarjeta de conductor	Tarjeta de control	Tarjeta de taller	Tarjeta de empresa
Ranura del segundo conductor	Sin tarjeta					
	Tarjeta de conductor				X	
	Tarjeta de control			X	X	X
	Tarjeta de taller		X	X	X	X
	Tarjeta de empresa			X	X	X

3.9.3 *Incidente «Solapamiento temporal»*

74) Este incidente se produce cuando la fecha/hora en que se extrajo por última vez una tarjeta de conductor, según quede registrado en dicha tarjeta, es posterior a la fecha/hora actual del aparato de control donde se inserta la tarjeta.

3.9.4 *Incidente «Conducción sin tarjeta adecuada»*

75) Este incidente se produce en determinadas combinaciones de dos tarjetas de tacógrafo válidas (indicadas con una X en el cuadro siguiente), cuando la actividad del conductor cambia a CONDUCCIÓN o cuando tiene lugar un cambio del modo de funcionamiento mientras la actividad del conductor es CONDUCCIÓN:

Conducción sin tarjeta adecuada		Ranura del conductor				
		Sin tarjeta (o tarjeta no válida)	Tarjeta de conductor	Tarjeta de control	Tarjeta de taller	Tarjeta de empresa
Ranura del segundo conductor	Sin tarjeta (o tarjeta no válida)	X		X		X
	Tarjeta de conductor	X		X	X	X
	Tarjeta de control	X	X	X	X	X
	Tarjeta de taller	X	X	X		X
	Tarjeta de empresa	X	X	X	X	X

3.9.5 *Incidente «Inserción de tarjeta durante la conducción»*

76) Este incidente se produce cuando se inserta una tarjeta de tacógrafo en una de las ranuras mientras la actividad del conductor es CONDUCCIÓN.

3.9.6 *Incidente «Error al cerrar la última sesión de la tarjeta»*

77) Este incidente se produce cuando, al insertar la tarjeta, el aparato de control detecta que, a pesar de lo dispuesto en el punto 3.1, la sesión anterior de la tarjeta no se ha cerrado correctamente (se ha extraído la tarjeta antes de que pudieran grabarse en ella todos los datos pertinentes). Este incidente afecta exclusivamente a las tarjetas de conductor y a las tarjetas de taller.

3.9.7 *Incidente «Exceso de velocidad»*

78) Este incidente se produce cada vez que se sobrepasa la velocidad permitida.

3.9.8 *Incidente «Interrupción del suministro eléctrico»*

79) Este incidente se produce cuando el suministro eléctrico del sensor de movimiento o de la unidad instalada en el vehículo se interrumpe durante más de 200 milisegundos, fuera del modo de calibrado o de control. El umbral de interrupción deberá definirlo el fabricante. La caída de tensión que se produce al arrancar el motor del vehículo no deberá activar este incidente.

3.9.9 *Incidente «Error de comunicación con el dispositivo de comunicación a distancia»*

80) Este incidente se produce, **fuera del modo de calibrado**, cuando el dispositivo de comunicación a distancia no acusa recibo de la correcta recepción de los datos de comunicación a distancia enviados desde la unidad instalada en el vehículo durante más de tres intentos.

3.9.10 *Incidente «Ausencia de información sobre la posición procedente del receptor GNSS»*

81) Este incidente se produce, **fuera del modo de calibrado**, en caso de ausencia de información sobre la posición procedente del receptor GNSS (sea interno o externo) durante más de tres horas de tiempo de conducción acumulado.

3.9.11 *Incidente «Error de comunicación con el dispositivo GNSS externo»*

82) Este incidente se produce, **fuera del modo de calibrado**, en caso de interrupción de la comunicación entre el receptor GNSS externo y la unidad instalada en el vehículo durante más de veinte minutos seguidos, cuando el vehículo está en movimiento.

3.9.12 *Incidente «Error de datos de movimiento»*

83) Este incidente se produce, **fuera del modo de calibrado**, en caso de interrupción del flujo normal de datos entre el sensor de movimiento y la unidad instalada en el vehículo o en caso de producirse un error de integridad o de autenticación de datos durante el intercambio entre el sensor de movimiento y la unidad instalada en el vehículo.

3.9.13 *Incidente «Conflicto de movimiento del vehículo»*

84) Este incidente se produce, **fuera del modo de calibrado**, en caso de que la información sobre el movimiento calculada a partir del sensor de movimiento esté en contradicción con la información sobre el movimiento calculada a partir del receptor GNSS interno o del dispositivo GNSS externo y eventualmente con otras fuentes independientes, tal como se especifica en el apéndice 12. Este incidente no debe producirse durante un trayecto en transbordador/tren o una condición «FUERA DE ÁMBITO», ni cuando no esté disponible la información sobre posición del receptor GNSS.

3.9.14 *Incidente «Intento de violación de la seguridad»*

85) Este incidente se produce cuando por algún motivo se ha visto afectada la seguridad del sensor de movimiento, de la unidad instalada en el vehículo o del dispositivo GNSS externo, según se especifica en el apéndice 10, fuera del modo de calibrado.

3.9.15 *Incidente «Conflicto temporal»*

86) Este incidente se produce cuando, **fuera del modo de calibrado**, la VU detecta una discrepancia de más de un minuto entre la hora de la función de medición de la hora de la unidad instalada en el vehículo y la hora procedente del receptor GNSS. Este incidente se registra junto con el valor del reloj interno de la unidad instalada en el vehículo y va acompañado de un ajuste de la hora automático. Después de haberse producido un incidente de conflicto temporal, la VU no generará más incidentes del mismo tipo durante las doce horas siguientes. Este incidente no se producirá cuando no hubiera una señal GNSS válida detectable por el receptor GNSS en los últimos treinta días. No obstante, cuando vuelva a estar disponible la información sobre la posición del receptor GNSS, se efectuará el ajuste de la hora automático.

3.9.16 *Fallo «Tarjeta»*

87) Este fallo está asociado al fallo de funcionamiento de una tarjeta de tacógrafo.

3.9.17 *Fallo «Aparato de control»*

88) Este fallo está asociado a uno de los fallos siguientes, fuera del modo de calibrado:

— fallo interno de la VU,

— fallo de la impresora,

— fallo de la pantalla,

— fallo de transferencia,

— fallo del sensor,

— fallo del receptor GNSS o del dispositivo GNSS externo,

— fallo del dispositivo de comunicación a distancia.

3.10 **Autodiagnóstico y comprobaciones automáticas**

89) El aparato de control deberá ser capaz de detectar los fallos ocurridos mediante comprobaciones automáticas y una función de autodiagnóstico, con arreglo al cuadro siguiente:

Subconjunto que se verifica	Comprobación automática	Autodiagnóstico
Software		Integridad
Memoria de datos	Acceso	Acceso, integridad de los datos
Dispositivos de interfaz para tarjetas	Acceso	Acceso
Teclado		Comprobación manual
Impresora	(depende del fabricante)	Documento impreso
Pantalla		Comprobación visual
Transferencia (exclusivamente durante la transferencia)	Funcionamiento correcto	
Sensor	Funcionamiento correcto	Funcionamiento correcto
Dispositivo de comunicación a distancia.	Funcionamiento correcto	Funcionamiento correcto
Dispositivo GNSS	Funcionamiento correcto	Funcionamiento correcto

3.11 **Lectura de datos de la memoria**

90) El aparato de control deberá ser capaz de leer todos los datos almacenados en su memoria.

3.12 **Registro y almacenamiento de datos en la memoria**

A efectos del presente apartado:

— Por «365 días» se entienden 365 días civiles de actividad media de un conductor en un vehículo. Por actividad media diaria en un vehículo se entiende al menos 6 conductores o segundos conductores, 6 ciclos de inserción-extracción de tarjeta y 256 cambios de actividad. Por consiguiente, «365 días» incluyen al menos 2 190 (segundos) conductores, 2 190 ciclos de inserción-extracción de tarjeta y 93 440 cambios de actividad.

— El número medio de posiciones por día se define como al menos 6 posiciones en las que comienza el período de trabajo diario, 6 posiciones en las que el tiempo de conducción continua del conductor llega a un múltiplo de tres horas, y 6 posiciones en las que termina el período de trabajo diario, por lo que «365 días» incluyen al menos 6 570 posiciones.

— Las horas se registran con una resolución de un minuto, a menos que se especifique lo contrario.

— Las lecturas del cuentakilómetros se registran con una resolución de un kilómetro.

— Las velocidades se registran con una resolución de 1 km/h.

— Las posiciones (latitudes y longitudes) se registran en grados y minutos, con una resolución de 1/10 de minuto, con la exactitud del GNSS asociada y la hora de adquisición.

91) En las condiciones de homologación, los datos almacenados en la memoria de datos no deberán verse afectados por interrupciones del suministro eléctrico de menos de doce meses de duración. Además, los datos almacenados en el dispositivo de comunicación a distancia externo, tal como se definen en el apéndice 14, no deberán verse afectados por interrupciones del suministro eléctrico de menos de 28 días de duración.

92) El aparato de control deberá ser capaz de registrar y almacenar de forma implícita o explícita en su memoria de datos lo siguiente:

3.12.1 *Datos de identificación de los equipos*

3.12.1.1 Datos de identificación de la unidad instalada en el vehículo

93) El aparato de control deberá ser capaz de almacenar en su memoria de datos los siguientes datos de identificación de la unidad instalada en el vehículo:

— nombre del fabricante,

— dirección del fabricante,

— número de pieza,

— número de serie,

— generación de la VU,

— capacidad para utilizar las tarjetas de tacógrafo de primera generación,

— versión de *software*,

— fecha de instalación de la versión de *software*,

— año de fabricación del equipo,

— número de homologación.

94) El fabricante de la unidad instalada en el vehículo registra y almacena de manera permanente, sin posibilidad de alteración, los datos de identificación de dicha unidad, excepto los datos relacionados con el *software* y el número de homologación, que pueden cambiar en caso de actualizar el *software* y la capacidad para utilizar las tarjetas de tacógrafo de primera generación.

3.12.1.2 Datos de identificación del sensor de movimiento

95) El sensor de movimiento deberá ser capaz de almacenar en su memoria los siguientes datos de identificación:

— nombre del fabricante,

— número de serie,

— número de homologación,

— identificador del componente de seguridad integrado (por ejemplo, número de pieza del chip/procesador interno),

— identificador del sistema operativo (por ejemplo, versión de *software*).

96) El fabricante del sensor de movimiento registra y almacena en el propio sensor de manera permanente, sin posibilidad de alteración, los datos de identificación de dicho sensor.

97) La unidad instalada en el vehículo deberá ser capaz de registrar y almacenar en su memoria los siguientes datos, correspondientes a los últimos veinte emparejamientos de los sensores de movimiento (si se producen varios emparejamientos dentro de un día civil, solo se almacenarán el primero y el último del día).

Deberán almacenarse los datos siguientes para cada uno de estos emparejamientos:

— datos de identificación del sensor de movimiento:

— número de serie,

— número de homologación,

— datos de emparejamiento del sensor de movimiento:

— fecha del emparejamiento.

3.12.1.3 Datos de identificación de los sistemas mundiales de navegación por satélite

98) El dispositivo GNSS externo deberá ser capaz de almacenar en su memoria los siguientes datos de identificación:

— nombre del fabricante,

— número de serie,

— número de homologación,

— identificador del componente de seguridad integrado (por ejemplo, número de pieza del chip/procesador interno),

— identificador del sistema operativo (por ejemplo, versión de *software*).

99) El fabricante del dispositivo GNSS externo registra y almacena en el propio dispositivo de manera permanente, sin posibilidad de alteración, los datos de identificación.

100) La unidad instalada en el vehículo deberá ser capaz de registrar y almacenar en su memoria los siguientes datos, correspondientes a los últimos veinte acoplamientos de dispositivos GNSS externos (si se producen varios acoplamientos dentro de un día civil, solo se almacenarán el primero y el último del día).

Deberán almacenarse los datos siguientes para cada uno de estos acoplamientos:

— datos de identificación del dispositivo GNSS externo:

— número de serie,

— número de homologación,

— datos de acoplamiento del dispositivo GNSS externo:

— fecha de acoplamiento.

3.12.2 *Claves y certificados*

101) El aparato de control deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte A y parte B.

3.12.3 *Datos de inserción y extracción de la tarjeta de conductor o de la tarjeta de taller*

102) Por cada ciclo de inserción y extracción de una tarjeta de conductor o una tarjeta de taller, el aparato de control deberá registrar y almacenar en su memoria de datos:

— el nombre y apellidos del titular de la tarjeta, tal y como constan en la tarjeta,

— el número de la tarjeta, el Estado miembro que la ha expedido y su fecha de expiración, tal y como constan en la tarjeta,

— la generación de la tarjeta,

— la fecha y hora de inserción,

— la lectura del cuentakilómetros del vehículo en el momento de insertar la tarjeta,

— la ranura donde se inserta la tarjeta,

— la fecha y hora de extracción,

— la lectura del cuentakilómetros del vehículo en el momento de extraer la tarjeta,

— la información siguiente acerca del vehículo anterior que utilizara el conductor, tal y como consta en la tarjeta:

— VRN y Estado miembro donde se matriculó el vehículo,

— generación de la VU (si está disponible),

— fecha y hora de extracción de la tarjeta,

— una bandera que indique si, en el momento de insertar la tarjeta, el titular ha introducido manualmente alguna actividad.

103) La memoria de datos deberá ser capaz de mantener estos datos almacenados durante al menos 365 días.

104) Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

3.12.4 *Datos sobre la actividad del conductor*

105) Cada vez que cambie la actividad del conductor o del segundo conductor, o cada vez que cambie el régimen de conducción, o cada vez que se inserte o extraiga una tarjeta de conductor o una tarjeta de taller, el aparato de control deberá registrar y almacenar en su memoria de datos:

— el régimen de conducción (EN EQUIPO, EN SOLITARIO),

— la ranura (CONDUCTOR, SEGUNDO CONDUCTOR),

— el estado de la tarjeta en la ranura que corresponda (INSERTADA, NO INSERTADA),

— la actividad (CONDUCCIÓN, DISPONIBILIDAD, TRABAJO, PAUSA/DESCANSO),

— la fecha y hora del cambio.

INSERTADA significa que se ha insertado en la ranura una tarjeta de conductor o una tarjeta de taller válidas. NO INSERTADA significa lo contrario, es decir, que no se ha insertado en la ranura una tarjeta de conductor o una tarjeta de taller válidas (por ejemplo, se inserta una tarjeta de empresa o no se inserta tarjeta).

Los datos de actividad que introduzca manualmente el conductor no se registran en la memoria de datos.

106) La memoria de datos deberá ser capaz de mantener estos datos almacenados durante al menos 365 días.

107) Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

3.12.5 *Lugares y posiciones donde comienzan o terminan los períodos de trabajo diarios y/o donde se alcanzan las tres horas de tiempo de conducción continua*

108) El aparato de control deberá registrar y almacenar en su memoria de datos:

— los lugares y las posiciones en que el conductor y/o el segundo conductor comienzan su período de trabajo diario;

— las posiciones en que el tiempo de conducción continua del conductor llega a un múltiplo de tres horas;

— los lugares y las posiciones en que el conductor y/o el segundo conductor finalizan su período de trabajo diario.

109) Cuando la posición del vehículo no esté disponible a partir del receptor GNSS en esos momentos, el aparato de control utilizará la posición más reciente disponible, y la fecha y hora asociadas.

110) Junto con cada lugar y posición, el aparato de control deberá registrar y almacenar en su memoria de datos:

— el número de tarjeta del (segundo) conductor y el Estado miembro que haya expedido la tarjeta,

— la generación de la tarjeta,

— la fecha y hora de la entrada,

— el tipo de entrada (comienzo, final o tres horas de tiempo de conducción continua),

— la exactitud, la fecha y la hora del GNSS, si procede,

— la lectura del cuentakilómetros del vehículo.

111) La memoria de datos deberá ser capaz de mantener almacenados durante al menos 365 días los lugares y posiciones en que comienzan o finalizan los períodos de trabajo diarios y/o se alcanzan las tres horas de tiempo de conducción continua.

112) Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

3.12.6 *Datos del cuentakilómetros*

113) Cada día civil a medianoche, el aparato de control deberá registrar en su memoria la lectura del cuentakilómetros del vehículo y la fecha correspondiente.

114) La memoria de datos deberá ser capaz de almacenar las lecturas de los cuentakilómetros a medianoche durante al menos 365 días civiles.

115) Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

3.12.7 *Datos pormenorizados sobre la velocidad*

116) Para cada segundo de al menos las últimas 24 horas en que haya estado en movimiento el vehículo, el aparato de control deberá registrar y almacenar en su memoria de datos la velocidad instantánea del vehículo y la fecha y hora correspondientes.

3.12.8 *Datos sobre incidentes*

A efectos del presente subapartado, la hora se registrará con una resolución de un segundo.

117) El aparato de control deberá registrar y almacenar en su memoria los datos siguientes para cada incidente detectado, con arreglo a las reglas de almacenamiento descritas a continuación:

Incidente	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
Inserción de una tarjeta no válida	— los diez incidentes más recientes.	— fecha y hora del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de la tarjeta que creó el incidente, — número de incidentes similares ocurridos ese día.
Conflicto de tarjetas	— los diez incidentes más recientes.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de las dos tarjetas que crearon el conflicto.
Conducción sin tarjeta adecuada	— el incidente de mayor duración ocurrido cada uno de los últimos diez días en que se hayan producido incidentes de este tipo, — los cinco incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.

Incidente	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
Inserción de tarjeta durante la conducción	— el último incidente ocurrido en cada uno de los diez últimos días en que se hayan producido incidentes de ese tipo,	— fecha y hora del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación, — número de incidentes similares ocurridos ese día.
Error al cerrar la última sesión de la tarjeta	— los diez incidentes más recientes.	— fecha y hora de inserción de la tarjeta, — tipo de tarjeta(s), número, Estado miembro emisor y generación, — datos de la última sesión según la lectura de la tarjeta: — fecha y hora de inserción de la tarjeta, — VRN, Estado miembro de matriculación y generación de la VU.
Exceso de velocidad (1)	— el incidente más grave en cada uno de los diez últimos días en que se hayan producido incidentes de este tipo (es decir, el que haya ocurrido con la velocidad media más alta), — los cinco incidentes más graves ocurridos en los últimos 365 días, — el primer incidente que haya ocurrido después del último calibrado.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — velocidad máxima medida durante el incidente, — media aritmética de la velocidad medida durante el incidente, — tipo de tarjeta, número, Estado miembro emisor y generación de la tarjeta del conductor (si procede), — número de incidentes similares ocurridos ese día.
Interrupción del suministro eléctrico (2)	— el incidente de mayor duración ocurrido cada uno de los últimos diez días en que se hayan producido incidentes de este tipo, — los cinco incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.
Error de comunicación con el dispositivo de comunicación a distancia	— el incidente de mayor duración ocurrido cada uno de los últimos diez días en que se hayan producido incidentes de este tipo, — los cinco incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.
Ausencia de información sobre la posición procedente del receptor GNSS	— el incidente de mayor duración ocurrido cada uno de los últimos diez días en que se hayan producido incidentes de este tipo, — los cinco incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.

Incidente	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
Error en datos de movimiento	— el incidente de mayor duración ocurrido cada uno de los últimos diez días en que se hayan producido incidentes de este tipo, — los cinco incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.
Conflicto de movimiento del vehículo	— el incidente de mayor duración ocurrido cada uno de los últimos diez días en que se hayan producido incidentes de este tipo, — los cinco incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora de comienzo del incidente, — fecha y hora de finalización del incidente, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.
Intento de violación de la seguridad	— los diez incidentes más recientes de cada tipo.	— fecha y hora de comienzo del incidente, — fecha y hora en que terminó el incidente (si es pertinente), — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — tipo de incidente.
Conflicto temporal	— el incidente de mayor duración ocurrido cada uno de los últimos diez días en que se hayan producido incidentes de este tipo, — los cinco incidentes de mayor duración ocurridos en los últimos 365 días.	— fecha y hora del aparato de control, — fecha y hora del GNSS, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el incidente, — número de incidentes similares ocurridos ese día.

(1) El aparato de control deberá registrar y almacenar también en su memoria de datos:

— la fecha y la hora del último CONTROL DEL EXCESO DE VELOCIDAD,

— la fecha y la hora del primer exceso de velocidad ocurrido tras este CONTROL DEL EXCESO DE VELOCIDAD,

— el número de incidentes de exceso de velocidad ocurridos después del último CONTROL DEL EXCESO DE VELOCIDAD.

(2) Estos datos solo podrán registrarse al reconectar la alimentación eléctrica. Las horas se determinarán con una precisión de un minuto.

3.12.9 *Datos sobre fallos*

A efectos del presente subapartado, la hora se registrará con una resolución de un segundo.

118) El aparato de control intentará registrar y almacenar en su memoria los datos siguientes para cada fallo detectado, con arreglo a las reglas de almacenamiento descritas a continuación:

Fallo	Reglas de almacenamiento	Datos que hay que registrar en cada fallo
Fallo de la tarjeta	— los diez fallos más recientes de la tarjeta de conductor.	— fecha y hora en que comenzó el fallo, — fecha y hora en que terminó el fallo, — tipo de tarjeta(s), número, Estado miembro emisor y generación.
Fallos del aparato de control	— los diez fallos más recientes de cada tipo, — el primer fallo ocurrido después del último calibrado.	— fecha y hora en que comenzó el fallo, — fecha y hora en que terminó el fallo, — tipo de fallo, — tipo de tarjeta(s), número, Estado miembro emisor y generación de cualquier tarjeta insertada al comenzar o al terminar el fallo.

3.12.10 *Datos de calibrado*

119) El aparato de control deberá registrar y almacenar en su memoria los datos correspondientes a:

— los parámetros de calibrado conocidos en el momento de la activación,

— su primer calibrado después de la activación,

— su primer calibrado en el vehículo actual (según conste en el VIN),

— los veinte calibrados más recientes (si el aparato se ha calibrado más de una vez en un mismo día civil, solo se almacenarán los datos correspondientes al primero y al último calibrados del día).

120) Cada vez que se calibre el aparato de control, se registrarán los datos siguientes:

— propósito del calibrado (activación, primera instalación, instalación, control periódico),

— nombre y dirección del taller,

— número de la tarjeta de taller, Estado miembro que haya expedido la tarjeta y fecha de expiración de la tarjeta,

— identificación del vehículo,

— parámetros que se actualizan o confirman: w, k, l, tamaño de los neumáticos, valor de ajuste del dispositivo limitador de la velocidad, cuentakilómetros (lectura anterior y nueva lectura), fecha y hora (valor anterior y nuevo valor),

— los tipos y los identificadores de todos los precintos existentes.

121) Además, el aparato de control deberá registrar y almacenar en su memoria de datos su capacidad para utilizar tarjetas de tacógrafo de primera generación (aún activada o no).

122) El sensor de movimiento deberá registrar y almacenar en su memoria los siguientes datos sobre la instalación del sensor de movimiento:

— primer emparejamiento con una VU (fecha, hora, número de homologación de la VU, número de serie de la VU),

— último emparejamiento con una VU (fecha, hora, número de homologación de la VU, número de serie de la VU).

123) El dispositivo GNSS externo deberá registrar y almacenar en su memoria los siguientes datos sobre la instalación del dispositivo GNSS externo:

— primer acoplamiento con una VU (fecha, hora, número de homologación de la VU, número de serie de la VU),

— último acoplamiento con una VU (fecha, hora, número de homologación de la VU, número de serie de la VU).

3.12.11 *Datos de ajuste de la hora*

124) El aparato de control deberá registrar y almacenar en su memoria los datos correspondientes a los ajustes de hora que se hayan realizado en el modo de calibrado y fuera del marco de un calibrado regular (def. f)):

— la última ocasión en que se ajustara la hora,

— los cinco casos en que el ajuste fuera mayor.

125) Cada vez que se ajuste la hora, se registrarán los datos siguientes:

— fecha y hora, valor anterior,

— fecha y hora, nuevo valor,

— nombre y dirección del taller,

— número de la tarjeta de taller, Estado miembro que haya expedido la tarjeta, generación de la tarjeta y fecha de expiración de la tarjeta.

3.12.12 *Datos sobre actividades de control*

126) El aparato de control deberá registrar y almacenar en su memoria los siguientes datos correspondientes a las veinte actividades de control más recientes:

— fecha y hora del control,

— número de la tarjeta de control, Estado miembro que haya expedido la tarjeta y generación de la tarjeta,

— tipo de control (visualización y/o impresión y/o transferencia de los datos de la VU y/o transferencia de los datos de la tarjeta y/o control del calibrado en carretera).

127) En caso de transferencia, también habrá que registrar las fechas correspondientes a los días transferidos más antiguos y más recientes.

3.12.13 *Datos sobre los bloqueos introducidos por las empresas*

128) El aparato de control deberá registrar y almacenar en su memoria los siguientes datos correspondientes a los 255 últimos bloqueos introducidos por una empresa:

— fecha y hora de activación del bloqueo,

— fecha y hora de desactivación del bloqueo,

— número de la tarjeta de empresa, Estado miembro que haya expedido la tarjeta y generación de la tarjeta,

— nombre y dirección de la empresa.

Los datos previamente bloqueados mediante un bloqueo eliminado de la memoria debido al límite antes mencionado se considerarán desbloqueados.

3.12.14 *Datos sobre actividades de transferencia*

129) El aparato de control deberá registrar y almacenar en su memoria los siguientes datos correspondientes a la última transferencia de datos de la memoria a medios externos, estando en el modo de empresa o en el modo de calibrado:

— fecha y hora de la transferencia,

— número de la tarjeta de empresa o de taller, Estado miembro que haya expedido la tarjeta y generación de la tarjeta,

— nombre de la empresa o del taller.

3.12.15 *Datos sobre condiciones específicas*

130) El aparato de control deberá registrar en su memoria los siguientes datos correspondientes a condiciones específicas:

— fecha y hora de la entrada,

— tipo de condición específica.

131) La memoria deberá ser capaz de mantener estos datos almacenados durante al menos 365 días (suponiendo que, como media, cada día se abra y se cierre una condición). Cuando se agote la capacidad de almacenamiento, los datos más antiguos se sustituirán por otros nuevos.

3.12.16 *Datos de la tarjeta de tacógrafo*

132) El aparato de control deberá ser capaz de almacenar los siguientes datos relativos a las diferentes tarjetas de tacógrafo que se han utilizado en la VU:

— número de la tarjeta de tacógrafo y su número de serie,

— fabricante de la tarjeta de tacógrafo,

— tipo de tarjeta de tacógrafo,

— versión de la tarjeta de tacógrafo.

133) El aparato de control deberá ser capaz de almacenar al menos 88 de estos registros.

3.13 **Lectura de las tarjetas de tacógrafo**

134) El aparato de control deberá ser capaz de leer las tarjetas de tacógrafo de primera y segunda generación para obtener, cuando proceda, los datos necesarios para:

— identificar el tipo de tarjeta, al titular de la tarjeta, el anterior vehículo empleado, la fecha y hora en que se retirara la tarjeta por última vez y la actividad seleccionada entonces,

— comprobar que la última sesión de la tarjeta se cerró correctamente,

— calcular el tiempo de conducción continua del conductor, su tiempo de descanso acumulado y sus tiempos de conducción acumulados durante la semana anterior y la actual,

— imprimir, previa solicitud, los datos registrados en una tarjeta de conductor,

— transferir a medios externos la información contenida en una tarjeta de conductor.

Este requisito solo se aplica a las tarjetas de tacógrafo de primera generación, siempre que su utilización no haya sido suprimida por un taller.

135) En caso de producirse un error de lectura, el aparato de control intentará ejecutar de nuevo el mismo comando de lectura. Si no lo consigue después de tres intentos, declarará la tarjeta defectuosa y no válida.

3.14 **Registro y almacenamiento de datos en las tarjetas de tacógrafo**

3.14.1 *Registro y almacenamiento de datos en las tarjetas de tacógrafo de primera generación*

136) Siempre que un taller no haya suprimido el uso de las tarjetas de tacógrafo de primera generación, el aparato de control deberá registrar y almacenar datos exactamente de la misma manera que lo haría un aparato de control de primera generación.

137) Nada más insertada la tarjeta de conductor o de taller, el aparato de control deberá configurar los «datos de la sesión» en dicha tarjeta.

138) El aparato de control deberá actualizar los datos almacenados en las tarjetas de conductor, de taller, de empresa o de control, si son válidas. Para ello, escribirá en la tarjeta todos los datos necesarios del titular correspondientes al período en que dicha tarjeta esté insertada. En el capítulo 4 se especifican los datos almacenados en cada tipo de tarjeta.

139) El aparato de control deberá actualizar los datos sobre la actividad del conductor y sobre los lugares (según se especifica en los puntos 4.5.3.1.9 y 4.5.3.1.11). Estos datos, almacenados en las tarjetas de conductor o en las tarjetas de taller, se sustituirán por los datos introducidos manualmente por el titular de la tarjeta.

140) Los incidentes no definidos para los aparatos de control de primera generación no se almacenarán en las tarjetas de conductor ni de taller.

141) Los datos de las tarjetas de tacógrafo se actualizarán de manera que, cuando sea necesario y teniendo en cuenta la capacidad real de almacenamiento de la tarjeta, los datos más recientes sustituyan a los más antiguos.

142) En caso de producirse un error de escritura, el aparato de control intentará ejecutar de nuevo el mismo comando de escritura. Si no lo consigue después de tres intentos, declarará la tarjeta defectuosa y no válida.

143) Antes de liberar una tarjeta de conductor, y después de haber almacenado en ella todos los datos pertinentes, el aparato de control deberá reiniciar los «datos de la sesión».

3.14.2 *Registro y almacenamiento de datos en las tarjetas de tacógrafo de segunda generación*

144) Las tarjetas de tacógrafo de segunda generación deberán incluir dos aplicaciones de tarjeta diferentes, la primero de las cuales será exactamente la misma que la aplicación TACHO de las tarjetas de tacógrafo de primera generación, y la segunda la aplicación TACHO_G2, que se especifica en el capítulo 4 y el apéndice 2.

145) Nada más insertada la tarjeta de conductor o de taller, el aparato de control deberá configurar los «datos de la sesión» en dicha tarjeta.

146) El aparato de control deberá actualizar los datos almacenados en las dos aplicaciones de las tarjetas de conductor, de taller, de empresa o de control, si son válidas. Para ello, escribirá en la tarjeta todos los datos necesarios del titular correspondientes al período en que dicha tarjeta esté insertada. En el capítulo 4 se especifican los datos almacenados en cada tipo de tarjeta.

147) El aparato de control deberá actualizar los datos sobre los lugares y posiciones de actividad del conductor (según se especifica en los puntos 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 y 4.5.3.2.11). Estos datos, almacenados en las tarjetas de conductor o en las tarjetas de taller válidas, se sustituirán por los datos de lugares de actividad introducidos manualmente por el titular de la tarjeta.

148) Los datos de las tarjetas de tacógrafo se actualizarán de manera que, cuando sea necesario y teniendo en cuenta la capacidad real de almacenamiento de la tarjeta, los datos más recientes sustituyan a los más antiguos.

149) En caso de producirse un error de escritura, el aparato de control intentará ejecutar de nuevo el mismo comando de escritura. Si no lo consigue después de tres intentos, declarará la tarjeta defectuosa y no válida.

150) Antes de liberar una tarjeta de conductor, y después de haber almacenado en las dos aplicaciones de la tarjeta todos los datos pertinentes, el aparato de control deberá reiniciar los «datos de la sesión».

3.15 **Visualización**

151) La pantalla deberá incluir al menos veinte caracteres.

152) Los caracteres tendrán un tamaño mínimo de 5 mm de alto y 3,5 mm de ancho.

153) La pantalla admitirá el uso de los caracteres especificados en el apéndice 1, Capítulo 4: «Conjuntos de caracteres». La pantalla podrá utilizar glifos simplificados (p.ej.: los caracteres acentuados podrán aparecer sin acento, o las minúsculas podrán verse como mayúsculas).

154) La pantalla deberá tener una iluminación adecuada que no provoque deslumbramiento.

155) Las indicaciones deberán ser visibles desde fuera del aparato de control.

156) El aparato de control deberá ser capaz de mostrar en pantalla:

— los datos por defecto,

— los datos relacionados con advertencias,

— los datos relacionados con el acceso a los menús,

— otros datos que solicite un usuario.

El aparato de control también podrá mostrar en pantalla otras informaciones, siempre que puedan distinguirse claramente de las arriba exigidas.

157) La pantalla del aparato de control deberá utilizar los pictogramas o las combinaciones de pictogramas enumerados en el apéndice 3. También podrán utilizarse otros pictogramas o combinaciones de pictogramas siempre que puedan distinguirse claramente de los exigidos.

158) La pantalla deberá estar siempre encendida (ON) cuando el vehículo esté en movimiento.

159) El aparato de control podrá incluir una función manual o automática que apague (OFF) la pantalla cuando el vehículo esté parado.

El formato de visualización se especifica en el apéndice 5.

3.15.1 *Contenido de la pantalla por defecto*

160) Cuando no sea necesario mostrar otra información, el aparato de control deberá presentar en pantalla, por defecto, los datos siguientes:

— la hora local (correspondiente a la UTC + desfase configurado por el conductor),

— el modo de funcionamiento,

— la actividad actual del conductor y la del segundo conductor,

— información relativa al conductor:

— si su actividad actual es CONDUCCIÓN, el tiempo actual de conducción continua y el tiempo actual de descanso acumulado hasta ese momento,

— si su actividad actual no es CONDUCCIÓN, la duración actual de su actividad (desde que la haya seleccionado) y el tiempo actual de descanso acumulado hasta ese momento.

161) La presentación en pantalla de los datos relativos a cada conductor será clara, sencilla e inequívoca. Si no fuera posible mostrar en pantalla simultáneamente la información relativa al conductor y la relativa al segundo conductor, el aparato de control deberá mostrar por defecto la información relativa al conductor y ofrecerá al usuario la posibilidad de visualizar la información relativa al segundo conductor.

162) Si el ancho de la pantalla no permite visualizar por defecto el modo de funcionamiento, el aparato de control mostrará unos instantes el nuevo modo de funcionamiento cuando cambie.

163) El aparato de control mostrará unos instantes el nombre del titular de la tarjeta en el momento de insertar la tarjeta.

164) Cuando se abra una condición «FUERA DE ÁMBITO» o «TRAYECTO EN TRANSBORDADOR/TREN», el contenido de la pantalla por defecto deberá mostrar, con el pictograma correspondiente, que la condición está abierta (se admite que no aparezca simultáneamente en pantalla la actividad actual del conductor).

3.15.2 *Visualización de advertencias*

165) Para las advertencias que muestre en pantalla el aparato de control se utilizarán principalmente los pictogramas del apéndice 3, completados cuando sea necesario por información adicional codificada en forma numérica. También se podrá añadir una descripción literal de la advertencia en el idioma preferido del conductor.

3.15.3 *Acceso mediante menús*

166) El aparato de control ofrecerá los comandos necesarios a través de una estructura de menús adecuada.

3.15.4 *Otras informaciones en pantalla*

167) Se podrán visualizar en pantalla, de manera selectiva y a voluntad, los siguientes datos:

— la fecha y la hora UTC, junto con el desfase horario local,

— el contenido de cualquiera de los siete documentos impresos, con el mismo formato que el propio documento,

— el tiempo de conducción continua y el tiempo de descanso acumulado del conductor,

— el tiempo de conducción continua y el tiempo de descanso acumulado del segundo conductor,

— el tiempo de conducción acumulado del conductor durante la semana anterior y la actual, y

— el tiempo de conducción acumulado del segundo conductor durante la semana anterior y la actual.

Datos opcionales:

— la duración actual de la actividad del segundo conductor (desde que la seleccionara),

— el tiempo de conducción acumulado del conductor durante la semana actual,

— el tiempo de conducción acumulado del segundo conductor durante el período de trabajo diario actual,

— el tiempo de conducción acumulado del conductor durante el período de trabajo diario actual.

168) El contenido del documento impreso se mostrará en pantalla de manera secuencial, línea por línea. Si el ancho de la pantalla es menor de 24 caracteres, el usuario dispondrá de un medio adecuado para visualizar la información completa (varias líneas, desplazamiento del texto, …).

No es necesario que aparezcan en pantalla las líneas del documento impreso destinadas a informaciones manuscritas.

3.16 **Impresión**

169) El aparato de control deberá ser capaz de imprimir la información almacenada en su memoria o en las tarjetas de tacógrafo. Habrá al menos siete tipos de documentos de impresión:

— impresión diaria de las actividades del conductor almacenadas en la tarjeta,

— impresión diaria de las actividades del conductor almacenadas en la unidad instalada en el vehículo,

— impresión de incidentes y fallos almacenados en la tarjeta,

— impresión de incidentes y fallos almacenados en la unidad instalada en el vehículo,

— impresión de datos técnicos,

— impresión de excesos de velocidad,

— historial de los datos de la tarjeta de tacógrafo para una determinada VU (véase el capítulo 3.12.16).

Los pormenores relativos al formato y al contenido de estos documentos se especifican en el apéndice 4.

Es posible incluir datos adicionales al final de los documentos de impresión.

El aparato de control también podrá imprimir otros documentos, siempre que puedan distinguirse claramente de los siete arriba indicados.

170) La «impresión diaria de las actividades del conductor almacenadas en la tarjeta» y la «impresión de incidentes y fallos almacenados en la tarjeta» solo estarán disponibles cuando se inserte en el aparato de control una tarjeta de conductor o una tarjeta de taller. El aparato de control actualizará los datos almacenados en la tarjeta correspondiente antes de iniciar la impresión.

171) A fin de obtener la «impresión diaria de las actividades del conductor almacenadas en la tarjeta» o la «impresión de incidentes y fallos almacenados en la tarjeta», el aparato de control deberá:

— seleccionar automáticamente la tarjeta de conductor o la tarjeta de taller, si solo se ha insertado una de estas dos tarjetas,

— o bien ofrecer un comando para seleccionar la tarjeta de origen o seleccionar la tarjeta en la ranura del conductor, si en el aparato de control se han insertado las dos tarjetas.

172) La impresora deberá ser capaz de imprimir 24 caracteres por línea.

173) Los caracteres tendrán un tamaño mínimo de 2,1 mm de alto y 1,5 mm de ancho.

174) La impresora admitirá el uso de los caracteres especificados en el apéndice 1, capítulo 4: «Conjuntos de caracteres».

175) Las impresoras estarán diseñadas de tal forma que faciliten los documentos de impresión arriba mencionados con la definición necesaria para evitar ambigüedades en la lectura.

176) Los documentos de impresión conservarán sus dimensiones y registros en las condiciones normales de humedad (10-90 %) y temperatura.

177) El tipo de papel homologado utilizado por el aparato de control llevará la marca de homologación pertinente y la indicación del/de los tipo(s) de aparato de control con que se puede utilizar.

178) Si se mantienen las condiciones normales de almacenamiento en lo que respecta a intensidad luminosa, humedad y temperatura, los documento de impresión seguirán siendo claramente legibles e identificables durante al menos dos años.

179) Las impresiones se ajustarán, como mínimo, a las especificaciones de ensayo que figuran en el apéndice 9.

180) Además, deberá ser posible incluir en los citados documentos inscripciones adicionales hechas a mano, tales como la firma del conductor.

181) En caso de que se acabe el papel durante la impresión de un documento, al cargarse un nuevo rollo el aparato de control deberá reiniciar la impresión desde la primera línea o bien continuar la impresión incluyendo una referencia inequívoca a la parte ya impresa.

3.17 **Advertencias**

182) El aparato de control deberá avisar al conductor cuando detecte algún incidente o fallo.

183) La advertencia por un incidente de interrupción del suministro eléctrico podrá hacerse cuando se restablezca el suministro.

184) El aparato de control deberá avisar al conductor quince minutos antes y en el preciso instante en que se exceda el límite de tiempo de conducción continua permitido.

185) Las señales de advertencia serán visuales, aunque también se podrán instalar señales de tipo acústico.

186) Las señales de advertencia visuales deberán ser perfectamente reconocibles para el usuario, estarán ubicadas dentro del campo de visión del conductor y podrán leerse claramente tanto de día como de noche.

187) Los avisadores luminosos podrán estar incorporados en el aparato de control o separados de él.

188) En este último caso, el avisador mostrará una «T».

189) Las señales de advertencia tendrán una duración de al menos treinta segundos, a menos que el usuario las confirme pulsando una o más teclas específicas del aparato de control. Esta primera confirmación no hará que desaparezca la indicación en pantalla del motivo de la advertencia (véase el párrafo siguiente).

190) El motivo de la advertencia se indicará en la pantalla del aparato de control y permanecerá visible hasta que lo confirme el usuario mediante una tecla o un comando específico del aparato de control.

191) También podrán instalarse otras señales de advertencia, siempre que el conductor no las confunda con las que se han definido anteriormente.

3.18 **Transferencia de datos a medios externos**

192) El aparato de control, a petición del usuario, deberá ser capaz de transferir a medios de almacenamiento externos los datos contenidos en la memoria o en una tarjeta de conductor, utilizando para ello el conector de calibrado/transferencia. El aparato de control actualizará los datos almacenados en la tarjeta correspondiente antes de iniciar la transferencia.

193) Asimismo, y como característica opcional, el aparato de control podrá, en cualquier modo de funcionamiento, transferir datos por cualquier otro medio a una empresa autentificada a través de este canal. En tal caso, dicha transferencia estará sujeta a los derechos de acceso a los datos en el modo de empresa.

194) La transferencia no deberá alterar ni borrar los datos almacenados.

195) Las características de la interfaz eléctrica del conector de calibrado/transferencia se especifican en el apéndice 6.

196) Los protocolos de transferencia se especifican en el apéndice 7.

3.19 **Comunicación a distancia para controles de carretera selectivos**

197) Cuando el encendido esté activado, la unidad instalada en el vehículo deberá almacenar cada sesenta segundos en el dispositivo de comunicación a distancia los datos más recientes necesarios a efectos de los controles en carretera selectivos. Estos datos se cifrarán y firmarán según lo especificado en el apéndice 11 y el apéndice 14.

198) Los datos que deben ser controlados a distancia estarán disponibles para los lectores de comunicación a distancia mediante comunicaciones inalámbricas, tal como se especifica en el apéndice 14.

199) Los datos necesarios a efectos de los controles en carretera selectivos deberán estar relacionados con:

— el intento más reciente de violación de la seguridad,

— la interrupción más larga del suministro eléctrico,

— un fallo del sensor,

— un error en los datos de movimiento,

— un conflicto de movimiento del vehículo,

— la conducción sin tarjeta válida,

— la inserción de la tarjeta mientras se conduce,

— los datos de ajuste de la hora,

— los datos sobre el calibrado, incluidas las fechas de los dos registros de calibrado más recientes almacenados,

— el número de matrícula del vehículo,

— la velocidad registrada por el tacógrafo.

3.20 **Envío de datos a dispositivos externos adicionales**

200) El aparato de control podrá ir también equipado de interfaces normalizadas que permitan que un aparato externo utilice en modo operativo o de calibrado los datos registrados o producidos por el tacógrafo.

En el apéndice 13 se especifica y normaliza una interfaz ITS opcional. Podrán coexistir otras interfaces similares, siempre que se cumplan plenamente los requisitos del apéndice 13 en términos de lista mínima de datos, seguridad y consentimiento del conductor.

Se aplicarán los siguientes requisitos a los datos de ITS facilitados a través de esa interfaz:

— estos datos constituirán una selección de los datos existentes a partir del diccionario de datos del tacógrafo (apéndice 1),

— un subconjunto de esta selección de datos se identificará como «datos personales»,

— el subconjunto de «datos personales» solo estará disponible si está habilitado el consentimiento verificable del conductor, aceptando que sus datos personales puedan abandonar la red del vehículo,

— en cualquier momento, podrá habilitarse o inhabilitarse el consentimiento del conductor a través de comandos del menú, siempre que esté insertada la tarjeta de conductor,

— la selección y el subconjunto de datos se emitirán a través del protocolo inalámbrico Bluetooth en el radio de la cabina del vehículo, con una frecuencia de refresco de un minuto,

— el emparejamiento del dispositivo exterior con la interfaz ITS estará protegido por un PIN aleatorio y dedicado de al menos cuatro dígitos, registrado y disponible a través de la pantalla de cada unidad instalada en el vehículo,

— en ninguna circunstancia podrá la presencia de la interfaz ITS perturbar ni alterar el correcto funcionamiento y la seguridad de la unidad instalada en el vehículo.

También se podrán enviar otros datos, además de la selección de datos existentes, que se considera la lista mínima, siempre que no se puedan considerar datos personales.

El aparato de control deberá notificar a otros dispositivos externos el consentimiento del conductor.

Cuando el encendido del vehículo esté activado (ON), estos datos se enviarán de manera permanente.

201) La interfaz de conexión en serie especificada en el anexo 1B del Reglamento (CEE) n.º 3821/85, en su última versión modificada, podrá seguir equipando los tacógrafos a efectos de retrocompatibilidad. De todos modos, seguirá siendo necesario el consentimiento del conductor en caso de transmisión de datos personales.

3.21 **Calibrado**

202) La función de calibrado deberá permitir:

— el emparejamiento automático del sensor de movimiento con la VU,

— el acoplamiento automático del dispositivo GNSS externo con la VU, en su caso,

— la adaptación digital de la constante del aparato de control (k) al coeficiente característico del vehículo (w),

— el ajuste de la hora actual dentro del período de validez de la tarjeta de taller insertada,

— el ajuste de la lectura actual del cuentakilómetros,

— la actualización de los datos de identificación del sensor de movimiento que hay almacenados en la memoria de datos,

— la actualización, en su caso, de los datos de identificación del dispositivo GNSS externo que hay almacenados en la memoria de datos,

— la actualización de los tipos y los identificadores de todos los precintos existentes,

— la actualización o confirmación de otros parámetros que conozca el aparato de control: identificación del vehículo, w, l, tamaño de los neumáticos y valor de ajuste del dispositivo limitador de la velocidad, en su caso.

203) Además, la función de calibrado permitirá suprimir la utilización de las tarjetas de tacógrafo de primera generación en el aparato de control, siempre que se cumplan las condiciones especificadas en el apéndice 15.

204) El emparejamiento del sensor de movimiento con la VU deberá constar al menos de los siguientes pasos:

— actualización (si es preciso) de los datos relativos a la instalación del sensor de movimiento, almacenados en el propio sensor de movimiento,

— copia, en la memoria de datos de la VU, de los datos necesarios para la identificación del sensor de movimiento, almacenados en el propio sensor de movimiento.

205) El acoplamiento del dispositivo GNSS externo con la VU deberá constar al menos de los siguientes pasos:

— actualización (si es preciso) de los datos relativos al dispositivo GNSS externo almacenados en el propio dispositivo GNSS externo,

— copia, en la memoria de datos de la VU, de los datos necesarios para la identificación del dispositivo GNSS externo, almacenados en el propio dispositivo GNSS externo, incluido el número de serie de este dispositivo.

El acoplamiento irá seguido de la verificación de la información de posición GNSS.

206) La función de calibrado deberá ser capaz de introducir todos los datos necesarios a través del conector de calibrado/transferencia, de acuerdo con el protocolo de calibrado definido en el apéndice 8. La función de calibrado también podrá utilizar otros medios para introducir los datos necesarios.

3.22 **Control del calibrado en carretera**

207) La función de control de calibrado en carretera permitirá la lectura del número de serie del sensor de movimiento (posiblemente integrado en el adaptador) y el número de serie del dispositivo GNSS externo (cuando proceda) conectado a la unidad instalada en el vehículo, en el momento de la petición.

208) Esta lectura será posible al menos en la pantalla de la unidad instalada en el vehículo a través de comandos en los menús.

209) La función de control de calibrado en carretera también permitirá controlar la selección del modo I/O de la línea de señal I/O de calibrado especificada en el apéndice 6 a través de la interfaz de la línea K. Esto se llevará a cabo a través de ECUAdjustmentSession, tal como se especifica en el apéndice 8, sección 7, «Control de los impulsos de prueba — Unidad funcional para control de entrada/salida».

3.23 **Ajuste de la hora**

210) La función de ajuste de la hora deberá permitir el ajuste automático de la hora actual. En el aparato de control se utilizan dos fuentes para el ajuste de la hora: 1) el reloj interno de la VU, 2) el receptor GNSS.

211) La hora del reloj interno de la VU se reajustará automáticamente a intervalos de doce horas como máximo. Cuando este plazo haya expirado y no se disponga de señal GNSS, se fijará la hora tan pronto como la VU pueda acceder a una hora válida facilitada por el receptor GNSS, según las condiciones de encendido del vehículo. La referencia temporal para la fijación automática de la hora del reloj interno de la VU se derivará del receptor GNSS. Se producirá un incidente de conflicto temporal si la hora actual se desvía más de un (1) minuto de la información horaria suministrada por el receptor GNSS.

212) La función de ajuste de la hora deberá permitir también el ajuste de la hora actual, en el modo de calibrado.

3.24 **Características de funcionamiento**

213) La unidad instalada en el vehículo deberá funcionar perfectamente en el intervalo de temperaturas que va de – 20 °C a 70 °C, el dispositivo GNSS externo en el intervalo de – 20 °C a 70 °C, y el sensor de movimiento en el intervalo de – 40 °C a 135 °C. El contenido de la memoria de datos no se borrará aunque la temperatura descienda hasta – 40 °C.

214) El aparato de control deberá funcionar perfectamente en el intervalo higrométrico del 10 % al 90 %.

215) Los precintos utilizados en el tacógrafo digital deberán resistir las mismas condiciones aplicables a los componentes del tacógrafo en el que estén colocados.

216) El aparato de control deberá estar protegido frente a sobretensiones, inversiones de polaridad de la fuente de alimentación y cortocircuitos.

217) Los sensores de movimiento:

— reaccionarán a todo campo magnético que perturbe la detección de movimiento del vehículo; en estas circunstancias, la unidad instalada en el vehículo registrará y almacenará un fallo del sensor (requisito 88), o bien

— estarán dotados de un sensor protegido de los campos magnéticos o invulnerable a estos.

218) El aparato de control y el dispositivo GNSS externo deberán ajustarse a la reglamentación internacional UN ECE R10 y estar protegidos contra descargas electrostáticas y fluctuaciones de la tensión.

3.25 **Materiales**

219) Todos los elementos que formen parte del aparato de control deberán estar fabricados con materiales de estabilidad y resistencia mecánica suficientes y de características eléctricas y magnéticas invariables.

220) Para unas condiciones normales de utilización, todas las partes internas del aparato deberán estar protegidas contra la humedad y el polvo.

221) La unidad instalada en el vehículo y el dispositivo GNSS externo deberán tener el grado de protección IP 40 y el sensor de movimiento el grado de protección IP 64, según la norma IEC 60529:1989, incluidos A1:1999 y A2:2013.

222) El aparato de control deberá ser conforme a todas las especificaciones técnicas aplicables relativas al diseño ergonómico.

223) El aparato de control deberá estar protegido frente a daños accidentales.

3.26 **Marcas**

224) Si el aparato de control permite visualizar la lectura del cuentakilómetros y la velocidad del vehículo, en su pantalla deberán figurar las precisiones siguientes:

— junto a la cifra que indica la distancia, la unidad de medida de la distancia, indicada mediante la abreviatura «km»,

— junto a la cifra que indica la velocidad, la abreviatura «km/h».

El aparato de control también debe ser capaz de mostrar la velocidad en millas por hora, en cuyo caso la unidad de medición de la velocidad se indicará con la abreviatura «mph». El aparato de control también debe ser capaz de mostrar la distancia en millas, en cuyo caso la unidad de medición de la distancia se indicará con la abreviatura «mi».

225) Cada uno de los componentes del aparato de control deberá llevar una placa descriptiva con la información siguiente:

— nombre y dirección del fabricante del aparato,

— número de pieza del fabricante y año de fabricación del aparato,

— número de serie del aparato,

— marca de homologación del modelo de aparato de control.

226) Cuando el espacio físico disponible no baste para mostrar todas las informaciones mencionadas, en la placa descriptiva deberá figurar al menos: el nombre o el logotipo del fabricante y el número de pieza del aparato.

4 CONDICIONES DE FABRICACIÓN Y FUNCIONAMIENTO DE LAS TARJETAS DE TACÓGRAFO

4.1 **Datos visibles**

El anverso de la tarjeta contendrá:

227) la mención «Tarjeta de conductor» o «Tarjeta de control» o «Tarjeta de taller» o «Tarjeta de la empresa», en mayúsculas, en la lengua o lenguas oficiales del Estado miembro que expida la tarjeta, según el tipo de tarjeta;

228) el nombre del Estado miembro que expida la tarjeta (opcional);

229) el distintivo del Estado miembro que expida la tarjeta, impreso en negativo en un rectángulo azul rodeado de doce estrellas amarillas; los distintivos serán los siguientes:

B	Bélgica	LV	Letonia
BG	Bulgaria	L	Luxemburgo
CZ	República Checa	LT	Lituania
CY	Chipre	M	Malta
DK	Dinamarca	NL	Países Bajos

D EST	Alemania Estonia	A PL	Austria Polonia
GR	Grecia	P RO SK SLO	Portugal Rumanía Eslovaquia Eslovenia
E	España	FIN	Finlandia
F HR H	Francia Croacia Hungría	S	Suecia
IRL	Irlanda	UK	Reino Unido
I	Italia		

230) las informaciones específicas de la tarjeta expedida, que constarán del siguiente modo:

	Tarjeta de conductor	Tarjeta de control	Tarjeta de empresa o de taller
1.	apellido(s) del conductor	nombre del organismo de control	nombre de la empresa o del taller
2.	nombre(s) del conductor	apellido(s) del controlador (en su caso)	apellido(s) del titular de la tarjeta (en su caso)
3.	fecha de nacimiento del conductor	nombre(s) del controlador (en su caso)	nombre(s) del titular de la tarjeta (en su caso)
4.a	fecha de comienzo de validez de la tarjeta		
4.b	fecha de expiración de la tarjeta		
4.c	designación de la autoridad expedidora (puede figurar en el reverso)		
4.d	un número distinto del que se recoge en la rúbrica 5, que sea útil para la gestión de la tarjeta (opcional)		
5. a	número del permiso de conducir (en la fecha de expedición de la tarjeta de conductor)	—	—
5. b	Número de tarjeta		
6.	fotografía del conductor	fotografía del controlador (opcional)	fotografía del instalador (opcional)

	Tarjeta de conductor	Tarjeta de control	Tarjeta de empresa o de taller
7.	firma del titular (opcional)		
8.	lugar de residencia habitual, o dirección postal del titular (opcional)	dirección postal del organismo de control	dirección postal de la empresa o taller

231) las fechas deberán escribirse con el formato «dd/mm/aaaa» o bien «dd.mm.aaaa» (día, mes, año).

El reverso de la tarjeta contendrá:

232) una explicación de las rúbricas numeradas que aparecen en el anverso de la tarjeta;

233) con autorización expresa por escrito del titular, podrán incluirse también informaciones que no estén relacionadas con la gestión de la tarjeta, pero sin que con ello se modifique en modo alguno la utilización del modelo como tarjeta de tacógrafo.

234) Las tarjetas de tacógrafo deberán imprimirse con los siguientes colores de fondo predominantes:

— tarjeta del conductor: blanco,

— tarjeta de control: azul,

— tarjeta de taller: rojo,

— tarjeta de empresa: amarillo.

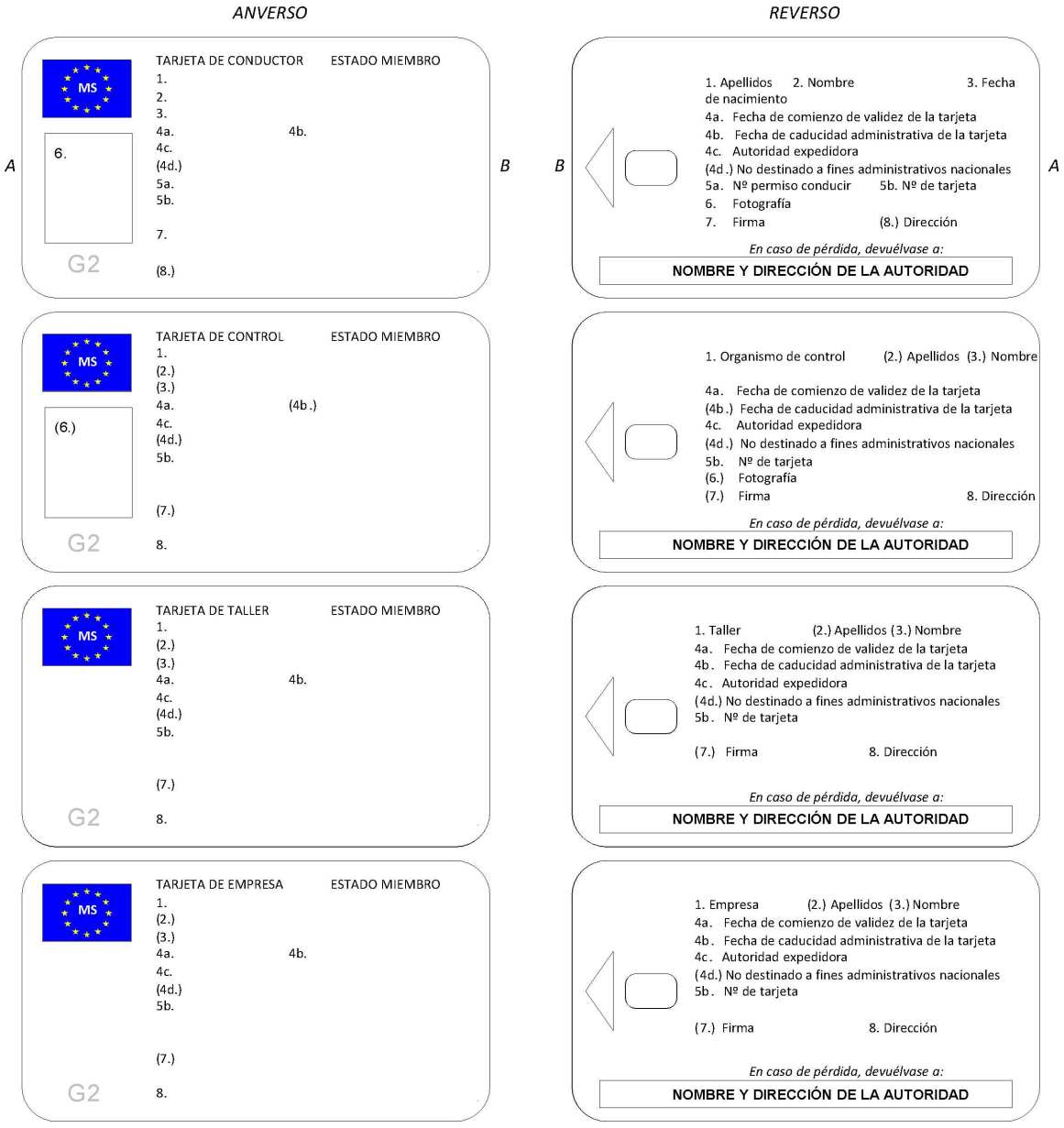
235) Las tarjetas de tacógrafo deberán reunir al menos las siguientes características de protección contra intentos de falsificación y manipulación:

— un fondo con diseño de seguridad, fondo labrado e impresión en arco iris,

— en la zona de la fotografía, el fondo con diseño de seguridad y la fotografía deberán solaparse,

— al menos una línea de microimpresión bicolor.

MODELO COMUNITARIO DE TARJETAS DE TACÓGRAFO



236) Previa consulta a la Comisión, los Estados miembros podrán añadir colores o inscripciones, tales como símbolos nacionales y características de seguridad, sin perjuicio de las demás disposiciones del presente anexo.

237) Las tarjetas temporales a que se refiere el artículo 26, apartado 4, del Reglamento (UE) n.º 165/2014 deberán cumplir lo dispuesto en el presente anexo.

4.2 Seguridad

La seguridad del sistema tiene por misión proteger la integridad y autenticidad de los datos que intercambian las tarjetas y el aparato de control, proteger la integridad y la autenticidad de los datos que se transfieren de las tarjetas, permitir determinadas operaciones de escritura en las tarjetas por parte del aparato de control exclusivamente, descifrar algunos datos, descartar toda posibilidad de falsificación de los datos almacenados en las tarjetas, impedir la manipulación y detectar todo intento en este sentido.

238) Al objeto de lograr la seguridad del sistema, las tarjetas de tacógrafo deberán cumplir los requisitos de seguridad que se definen en los apéndices 10 y 11.

239) Las tarjetas de tacógrafo podrán leerse con otros equipos, como por ejemplo ordenadores personales.

4.3 **Normas**

240) Las tarjetas de tacógrafo deberán ajustarse a las normas siguientes:

— ISO/IEC 7810 Tarjetas de identificación — Características físicas.

— ISO/IEC 7816 Tarjetas de identificación — Tarjetas con circuitos integrados,

— Parte 1: Características físicas,

— Parte 2: Dimensiones y ubicación de los contactos (ISO/IEC 7816-2:2007),

— Parte 3: Interfaz eléctrica y protocolos de transmisión (ISO/IEC 7816-3:2006),

— Parte 4: Organización, seguridad y comandos para los intercambios (ISO/IEC 7816-4:2013 + Cor 1:2014),

— Parte 6: Elementos de datos intersectoriales para los intercambios (ISO/IEC 7816-6:2004 + Cor 1:2006),

— Parte 8: Comandos para las operaciones de seguridad (ISO/IEC 7816-8: 2004).

— Las tarjetas de tacógrafo deberán someterse a ensayo con arreglo a la norma ISO/IEC 10373-3:2010 (Tarjetas de identificación — Métodos de ensayo — Parte 3: Tarjetas con circuitos integrados con contactos y dispositivos de interfaz conexos.

4.4 **Especificaciones ambientales y eléctricas**

241) Las tarjetas de tacógrafo deberán estar en condiciones de funcionar correctamente bajo cualquier condición climática habitual en el territorio de la Comunidad y al menos en el intervalo de temperaturas comprendido entre – 25 °C y + 70 °C, con picos ocasionales de hasta + 85 °C («ocasional» significa no más de cuatro horas cada vez y no más de cien veces durante la vida útil de la tarjeta).

242) Las tarjetas deberán poder funcionar correctamente en el intervalo de humedad comprendido entre el 10 % y el 90 %.

243) Las tarjetas de tacógrafo deberán poder funcionar correctamente durante cinco años si se utilizan con arreglo a las especificaciones ambientales y eléctricas.

244) Por lo que respecta a su funcionamiento, las tarjetas deberán ajustarse a ECE R10, en relación con la compatibilidad electromagnética, y deberán estar protegidas contra descargas electrostáticas.

4.5 **Almacenamiento de datos**

A efectos del presente apartado:

— las horas se registran con una resolución de un minuto, a menos que se especifique lo contrario,

— las lecturas del cuentakilómetros se registran con una resolución de un kilómetro,

— las velocidades se registran con una resolución de 1 km/h,

— las posiciones (latitudes y longitudes) se registran en grados y minutos, con una resolución de 1/10 de minuto.

Las funciones, comandos y estructuras lógicas de las tarjetas de tacógrafo, por lo que respecta al cumplimiento de las condiciones de almacenamiento de datos, se especifican en el apéndice 2.

Si no se especifica otra cosa, el almacenamiento de datos en las tarjetas de tacógrafo deberá organizarse de tal manera que los datos nuevos sustituyan a los datos más antiguos almacenados en caso de que el tamaño de la memoria prevista para los registros específicos se agote.

245) En este apartado se especifica la capacidad mínima de almacenamiento de los diferentes archivos de datos de la aplicación. Las tarjetas de tacógrafo deberán ser capaces de indicar al aparato de control la capacidad real de almacenamiento de dichos archivos.

246) Cualquier dato adicional que pueda almacenarse en una tarjeta de tacógrafo, relacionado con otras aplicaciones eventualmente alojadas en la tarjeta, deberá almacenarse de conformidad con la Directiva 95/46/CE, y con la Directiva 2002/58/CE, y dando cumplimiento al artículo 7 del Reglamento (UE) n.º 165/2014.

247) Cada archivo maestro (MF) de cualquier tarjeta de tacógrafo deberá contener hasta cinco archivos elementales (EF) referidos a la gestión de la tarjeta, identificaciones de la aplicación y del chip, y dos archivos dedicados (DF):

— DF Tachograph, que contiene la aplicación accesible a las unidades instaladas en vehículos de primera generación, que también está presente en las tarjetas de tacógrafo de primera generación,

— DF Tachograph_G2, que contiene la aplicación únicamente accesible a las unidades instaladas en vehículos de segunda generación, que solo está presente en las tarjetas de tacógrafo de segunda generación.

Los detalles de la estructura de las tarjetas de tacógrafo se especifican íntegramente en el apéndice 2.

4.5.1 *Archivos elementales para la identificación y la gestión de la tarjeta*

4.5.2 *Identificación de la tarjeta CI*

248) Las tarjetas de tacógrafo deberán ser capaces de almacenar los siguientes datos para la identificación de la tarjeta inteligente:

— parada de reloj,

— número de serie de la tarjeta (incluidas referencias de fabricación),

— número de homologación de la tarjeta,

— identificación personal de la tarjeta (ID),

— ID del integrador,

— identificador del CI.

4.5.2.1 Identificación del chip

249) Las tarjetas de tacógrafo deberán ser capaces de almacenar los siguientes datos para la identificación del circuito integrado (CI):

— número de serie del CI,

— referencias de fabricación del CI.

4.5.2.2 DIR (presente solo en las tarjetas de tacógrafo de segunda generación).

250) Las tarjetas de tacógrafo deberán ser capaces de almacenar los objetos de datos de identificación de la aplicación especificados en el apéndice 2.

4.5.2.3 Información ATR (condicionalmente, presente solo en las tarjetas de tacógrafo de segunda generación).

251) Las tarjetas de tacógrafo deberán ser capaces de almacenar el siguiente objeto de datos de información de longitud extendida:

— en el caso de que la tarjeta de tacógrafo acepte campos de longitud extendida, el objeto de datos de información de longitud extendida especificado en el apéndice 2.

4.5.2.4 Información de longitud extendida (condicionalmente, presente solo en las tarjetas de tacógrafo de segunda generación).

252) Las tarjetas de tacógrafo deberán ser capaces de almacenar los siguientes objetos de datos de información de longitud extendida:

— en el caso de que la tarjeta de tacógrafo acepte campos de longitud extendida, los objetos de datos de información de longitud extendida especificados en el apéndice 2.

4.5.3 *Tarjeta de conductor*

4.5.3.1 Aplicación del tacógrafo (accesible a las unidades instaladas en vehículos de primera y segunda generación)

4.5.3.1.1 Identificación de la aplicación

253) La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos de identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

4.5.3.1.2 Clave y certificados

254) La tarjeta de conductor deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte A.

4.5.3.1.3 Identificación de la tarjeta

255) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos de identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidieron la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de expiración de la tarjeta.

4.5.3.1.4 Identificación del titular de la tarjeta

256) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos de identificación del titular de la tarjeta:

— apellido(s) del titular,

— nombre(s) del titular,

— fecha de nacimiento,

— idioma preferido.

4.5.3.1.5 Transferencia de los datos de la tarjeta

257) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a las transferencias desde la tarjeta:

— fecha y hora de la última transferencia de los datos de la tarjeta (para fines distintos de los de control).

258) La tarjeta de conductor deberá ser capaz de mantener almacenado uno de dichos registros.

4.5.3.1.6 Información sobre el permiso de conducir

259) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos sobre el permiso de conducir:

— Estado miembro y autoridad que hayan expedido el permiso,

— número del permiso de conducir (en la fecha de expedición de la tarjeta).

4.5.3.1.7 Datos sobre incidentes

A efectos del presente subapartado, la hora se almacenará con una resolución de un segundo.

260) La tarjeta de conductor deberá ser capaz de almacenar los datos relativos a los siguientes incidentes detectados por el aparato de control con la tarjeta insertada:

— solapamiento temporal (cuando esa tarjeta sea la causa del incidente),

— inserción de la tarjeta durante la conducción (cuando esa tarjeta sea el objeto del incidente),

— error al cerrar la última sesión de la tarjeta (cuando esa tarjeta sea el objeto del incidente),

— interrupción del suministro eléctrico,

— error en datos de movimiento,

— intentos de violación de la seguridad:

261) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos sobre dichos incidentes:

— código del incidente,

— fecha y hora en que comenzó el incidente (o en que se insertó la tarjeta, si el incidente estaba ocurriendo en ese momento),

— fecha y hora en que terminó el incidente (o en que se extrajo la tarjeta, si el incidente estaba ocurriendo en ese momento),

— VRN y Estado miembro donde se matriculó el vehículo en el que ocurrió el incidente.

Nota: por lo que respecta al incidente de «solapamiento temporal»:

— la fecha y hora en que comenzó el incidente deberán coincidir con la fecha y hora en que se extrajo la tarjeta del vehículo anterior,

— la fecha y hora en que terminó el incidente deberán coincidir con la fecha y hora en que se insertó la tarjeta en el vehículo actual,

— los datos del vehículo deberán coincidir con los del vehículo en que se produce el incidente.

Nota: por lo que respecta al incidente de «error al cerrar la última sesión de la tarjeta»:

— la fecha y hora en que comenzó el incidente deberán coincidir con la fecha de inserción de la tarjeta y la hora de la sesión que no se cerró correctamente,

— la fecha y hora en que terminó el incidente deberán coincidir con la fecha de inserción de la tarjeta y la hora de la sesión durante la que se detectó el incidente (sesión actual),

— los datos del vehículo deberán coincidir con los del vehículo en que la sesión no se cerró correctamente.

262) La tarjeta de conductor deberá ser capaz de almacenar los datos correspondientes a los seis incidentes más recientes de cada tipo (es decir, un total de 36 incidentes).

4.5.3.1.8 Datos sobre fallos

A efectos del presente subapartado, la hora se registrará con una resolución de un segundo.

263) La tarjeta de conductor deberá ser capaz de almacenar los datos relativos a los siguientes fallos detectados por el aparato de control estando la tarjeta insertada:

— fallo de la tarjeta (cuando esa tarjeta sea el tema del incidente),

— fallo del aparato de control.

264) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos sobre dichos fallos:

— código de fallo,

— fecha y hora en que comenzó el fallo (o en que se insertó la tarjeta, si el fallo estaba ocurriendo en ese momento),

— fecha y hora en que terminó el fallo (o en que se extrajo la tarjeta, si el fallo estaba ocurriendo en ese momento),

— VRN y Estado miembro donde se matriculó el vehículo en el que ocurrió el fallo.

265) La tarjeta de conductor deberá ser capaz de almacenar los datos correspondientes a los doce fallos más recientes de cada tipo (es decir, un total de veinticuatro fallos).

4.5.3.1.9 Datos sobre la actividad del conductor

266) La tarjeta de conductor deberá ser capaz de almacenar, para cada día civil que se haya utilizado la tarjeta o para el cual el conductor haya introducido actividades manualmente, los siguientes datos:

— la fecha,

— un contador de presencia diaria (incrementado en una unidad por cada uno de estos días civiles),

— la distancia total recorrida por el conductor durante ese día,

— el régimen de conducción a las 00.00 horas,

— cada vez que el conductor cambie de actividad, o cambie el régimen de conducción, o inserte o extraiga su tarjeta:

  — el régimen de conducción (EN EQUIPO, EN SOLITARIO),

  — la ranura (CONDUCTOR, SEGUNDO CONDUCTOR),

  — el estado de la tarjeta (INSERTADA, NO INSERTADA),

  — la actividad (CONDUCCIÓN, DISPONIBILIDAD, TRABAJO, PAUSA/DESCANSO),

  — la hora del cambio.

267) La memoria de la tarjeta de conductor deberá ser capaz de mantener almacenados durante al menos veintiocho días los datos sobre la actividad del conductor (la actividad media de un conductor se define como 93 cambios de actividad por día).

268) Los datos enumerados en los requisitos 261, 264 y 266 deberán almacenarse de manera que las actividades puedan recuperarse en su orden de ocurrencia, incluso en una situación de solapamiento temporal.

4.5.3.1.10 Datos sobre vehículos empleados

269) La tarjeta de conductor deberá ser capaz de almacenar, para cada día civil que se haya utilizado la tarjeta y para cada período de uso del vehículo en ese día (un período de uso incluye todos los ciclos consecutivos de inserción/extracción de la tarjeta en el vehículo, visto desde el punto de vista de la tarjeta), los siguientes datos:

— fecha y hora en que se utiliza el vehículo por primera vez (es decir, primera inserción de la tarjeta en ese período de uso del vehículo, o bien 00.00 horas si el vehículo se está utilizando en ese momento),

— valor del cuentakilómetros del vehículo en ese momento,

— fecha y hora en que se utiliza el vehículo por última vez, (es decir, última extracción de la tarjeta en ese período de uso del vehículo, o bien 23.59 horas si el vehículo se está utilizando en ese momento),

— valor del cuentakilómetros del vehículo en ese momento,

— VRN y Estado miembro donde se matriculó el vehículo.

270) La tarjeta de conductor deberá ser capaz de almacenar al menos 84 de estos registros.

4.5.3.1.11 Lugares donde comienzan o terminan los períodos de trabajo diarios

271) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos, que introduce el conductor, relativos a los lugares donde comienzan o terminan los períodos de trabajo diarios:

— la fecha y hora de la introducción (o la fecha/hora relacionada con la introducción si esta tiene lugar durante el procedimiento de introducción manual),

— el tipo de introducción (comienzo o final, condición de introducción),

— el país y la región introducidos,

— la lectura del cuentakilómetros del vehículo.

272) La memoria de la tarjeta de conductor deberá ser capaz de mantener almacenados al menos 42 pares de estos registros.

4.5.3.1.12 Datos de la sesión

273) La tarjeta de conductor deberá ser capaz de almacenar los datos relativos al vehículo que abrió la sesión actual:

— fecha y hora en que se abrió la sesión (es decir, inserción de la tarjeta), con una resolución de un segundo,

— VRN y Estado miembro donde se matriculó el vehículo.

4.5.3.1.13 Datos sobre actividades de control

274) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a las actividades de control:

— fecha y hora del control,

— número de la tarjeta de control y Estado miembro que haya expedido la tarjeta,

— tipo de control (visualización o impresión o transferencia de los datos de la VU o transferencia de los datos de la tarjeta [véase la nota]),

— período transferido, en caso de transferencia,

— VRN y Estado miembro donde se matriculó el vehículo en el que se produjera el control.

Nota: la transferencia de los datos de la tarjeta solo quedará registrada si se lleva a cabo con un aparato de control.

275) La tarjeta de conductor deberá ser capaz de mantener almacenado uno de dichos registros.

4.5.3.1.14 Datos sobre condiciones específicas

276) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a las condiciones específicas que se introdujeron al insertar la tarjeta (en la ranura que fuese):

— fecha y hora de la introducción,

— tipo de condición específica.

277) La tarjeta de conductor deberá ser capaz de almacenar al menos 56 de estos registros.

4.5.3.2 Aplicación de tacógrafo de segunda generación (no accesible a la unidad instalada en el vehículo de primera generación)

4.5.3.2.1 Identificación de la aplicación

278) La tarjeta del conductor deberá ser capaz de almacenar los siguientes datos de identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

4.5.3.2.2 Claves y certificados

279) La tarjeta de conductor deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte B.

4.5.3.2.3 Identificación de la tarjeta

280) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos de identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidieron la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de expiración de la tarjeta.

4.5.3.2.4 Identificación del titular de la tarjeta

281) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos de identificación del titular de la tarjeta:

— apellido(s) del titular,

— nombre(s) del titular,

— fecha de nacimiento,

— idioma preferido.

4.5.3.2.5 Transferencia de los datos de la tarjeta

282) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a las transferencias desde la tarjeta:

— fecha y hora de la última transferencia de los datos de la tarjeta (para fines distintos de los de control).

283) La tarjeta de conductor deberá ser capaz de mantener almacenado uno de dichos registros.

4.5.3.2.6 Información sobre el permiso de conducir

284) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos sobre el permiso de conducir:

— Estado miembro y autoridad que hayan expedido el permiso,

— número del permiso de conducir (en la fecha de expedición de la tarjeta).

4.5.3.2.7 Datos sobre incidentes

A efectos del presente subapartado, la hora se almacenará con una resolución de un segundo.

285) La tarjeta de conductor deberá ser capaz de almacenar los datos relativos a los siguientes incidentes detectados por el aparato de control con la tarjeta insertada:

— solapamiento temporal (cuando esa tarjeta sea la causa del incidente),

— inserción de la tarjeta durante la conducción (cuando esa tarjeta sea el objeto del incidente),

— error al cerrar la última sesión de la tarjeta (cuando esa tarjeta sea el objeto del incidente),

— interrupción del suministro eléctrico,

— error de comunicación con el dispositivo de comunicación a distancia,

— ausencia de información sobre la posición procedente del receptor GNSS,

— error de comunicación con el dispositivo GNSS externo,

— error en datos de movimiento,

— conflicto de movimiento del vehículo,

— intentos de violación de la seguridad,

— conflicto temporal.

286) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos sobre dichos incidentes:

— código del incidente,

— fecha y hora en que comenzó el incidente (o en que se insertó la tarjeta, si el incidente estaba ocurriendo en ese momento),

— fecha y hora en que terminó el incidente (o en que se extrajo la tarjeta, si el incidente estaba ocurriendo en ese momento),

— VRN y Estado miembro donde se matriculó el vehículo en el que ocurrió el incidente.

Nota: por lo que respecta al incidente de «solapamiento temporal»:

— la fecha y hora en que comenzó el incidente deberán coincidir con la fecha y hora en que se extrajo la tarjeta del vehículo anterior,

— la fecha y hora en que terminó el incidente deberán coincidir con la fecha y hora en que se insertó la tarjeta en el vehículo actual,

— los datos del vehículo deberán coincidir con los del vehículo en que se produce el incidente.

Nota: por lo que respecta al incidente de «error al cerrar la última sesión de la tarjeta»:

— la fecha y hora en que comenzó el incidente deberán coincidir con la fecha de inserción de la tarjeta y la hora de la sesión que no se cerró correctamente,

— la fecha y hora en que terminó el incidente deberán coincidir con la fecha de inserción de la tarjeta y la hora de la sesión durante la que se detectó el incidente (sesión actual),

— los datos del vehículo deberán coincidir con los del vehículo en que la sesión no se cerró correctamente.

287) La tarjeta de conductor deberá ser capaz de almacenar los datos correspondientes a los seis incidentes más recientes de cada tipo (es decir, un total de 66 incidentes).

4.5.3.2.8 Datos sobre fallos

A efectos del presente subapartado, la hora se registrará con una resolución de un segundo.

288) La tarjeta de conductor deberá ser capaz de almacenar los datos relativos a los siguientes fallos detectados por el aparato de control estando la tarjeta insertada:

— fallo de la tarjeta (cuando esa tarjeta sea el tema del incidente),

— fallo del aparato de control.

289) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos sobre dichos fallos:

— código de fallo,

— fecha y hora en que comenzó el fallo (o en que se insertó la tarjeta, si el fallo estaba ocurriendo en ese momento),

— fecha y hora en que terminó el fallo (o en que se extrajo la tarjeta, si el fallo estaba ocurriendo en ese momento),

— VRN y Estado miembro donde se matriculó el vehículo en el que ocurrió el fallo.

290) La tarjeta de conductor deberá ser capaz de almacenar los datos correspondientes a los doce fallos más recientes de cada tipo (es decir, un total de veinticuatro fallos).

4.5.3.2.9 Datos sobre la actividad del conductor

291) La tarjeta de conductor deberá ser capaz de almacenar, para cada día civil que se haya utilizado la tarjeta o para el cual el conductor haya introducido actividades manualmente, los siguientes datos:

— la fecha,

— un contador de presencia diaria (incrementado en una unidad por cada uno de estos días civiles),

— la distancia total recorrida por el conductor durante ese día,

— el régimen de conducción a las 00.00 horas,

— cada vez que el conductor cambie de actividad, o cambie el régimen de conducción, o inserte o extraiga su tarjeta:

— el régimen de conducción (EN EQUIPO, EN SOLITARIO),

— la ranura (CONDUCTOR, SEGUNDO CONDUCTOR),

— el estado de la tarjeta (INSERTADA, NO INSERTADA),

— la actividad (CONDUCCIÓN, DISPONIBILIDAD, TRABAJO, PAUSA/DESCANSO),

— la hora del cambio.

292) La memoria de la tarjeta de conductor deberá ser capaz de mantener almacenados durante al menos veintiocho días los datos sobre la actividad del conductor (la actividad media de un conductor se define como 93 cambios de actividad por día).

293) Los datos enumerados en los requisitos 286, 289 y 291 deberán almacenarse de manera que las actividades puedan recuperarse en su orden de ocurrencia, incluso en una situación de solapamiento temporal.

4.5.3.2.10 Datos sobre vehículos empleados

294) La tarjeta de conductor deberá ser capaz de almacenar, para cada día civil que se haya utilizado la tarjeta y para cada período de uso del vehículo en ese día (un período de uso incluye todos los ciclos consecutivos de inserción/extracción de la tarjeta en el vehículo, visto desde el punto de vista de la tarjeta), los siguientes datos:

— fecha y hora en que se utiliza el vehículo por primera vez (es decir, primera inserción de la tarjeta en ese período de uso del vehículo, o bien 00.00 horas si el vehículo se está utilizando en ese momento),

— valor del cuentakilómetros del vehículo en ese momento de primer uso,

— fecha y hora en que se utiliza el vehículo por última vez, (es decir, última extracción de la tarjeta en ese período de uso del vehículo, o bien 23.59 horas si el vehículo se está utilizando en ese momento),

— valor del cuentakilómetros del vehículo en ese momento de último uso,

— VRN y Estado miembro donde se matriculó el vehículo,

— VIN del vehículo.

295) La tarjeta de conductor deberá ser capaz de almacenar al menos 84 de estos registros.

4.5.3.2.11 Lugares y posiciones donde comienzan o terminan los períodos de trabajo diarios

296) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos, que introduce el conductor, relativos a los lugares donde comienzan o terminan los períodos de trabajo diarios:

— la fecha y hora de la introducción (o la fecha/hora relacionada con la introducción si esta tiene lugar durante el procedimiento de introducción manual),

— el tipo de introducción (comienzo o final, condición de introducción),

— el país y la región introducidos,

— la lectura del cuentakilómetros del vehículo,

— la posición del vehículo,

— La exactitud del GNSS, fecha y hora en que se haya determinado la posición.

297) La memoria de la tarjeta de conductor deberá ser capaz de mantener almacenados al menos 84 pares de estos registros.

4.5.3.2.12 Datos de la sesión

298) La tarjeta de conductor deberá ser capaz de almacenar los datos relativos al vehículo que abrió la sesión actual:

— fecha y hora en que se abrió la sesión (es decir, inserción de la tarjeta), con una resolución de un segundo,

— VRN y Estado miembro donde se matriculó el vehículo.

4.5.3.2.13 Datos sobre actividades de control

299) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a las actividades de control:

— fecha y hora del control,

— número de la tarjeta de control y Estado miembro que haya expedido la tarjeta,

— tipo de control (visualización o impresión o transferencia de los datos de la VU o transferencia de los datos de la tarjeta [véase la nota]),

— período transferido, en caso de transferencia,

— VRN y Estado miembro donde se matriculó el vehículo en el que se produjera el control.

Nota: las condiciones de seguridad implican que la transferencia de los datos de la tarjeta solo quedará registrada si se lleva a cabo con un aparato de control.

300) La tarjeta de conductor deberá ser capaz de mantener almacenado uno de dichos registros.

4.5.3.2.14 Datos sobre condiciones específicas

301) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a las condiciones específicas que se introdujeron al insertar la tarjeta (en la ranura que fuese):

— fecha y hora de la introducción,

— tipo de condición específica.

302) La tarjeta de conductor deberá ser capaz de almacenar al menos 56 de estos registros.

4.5.3.2.15 Datos utilizados en unidades instaladas en vehículos

303) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a las diferentes unidades instaladas en vehículos en que se utilice la tarjeta:

— fecha y la hora en que comienza el período de uso de la unidad instalada en el vehículo (es decir, primera inserción de la tarjeta en la unidad instalada en el vehículo en el período),

— nombre del fabricante de la unidad instalada en el vehículo,

— tipo de unidad instalada en el vehículo,

— versión del *software* que lleva instalado la unidad instalada en el vehículo.

304) La tarjeta de conductor deberá ser capaz de almacenar al menos 84 de estos registros.

4.5.3.2.16 Datos sobre lugares en tres horas de conducción continua

305) La tarjeta de conductor deberá ser capaz de almacenar los siguientes datos relativos a la posición del vehículo cuando el tiempo de conducción continua del conductor alcance un múltiplo de tres horas:

— fecha y hora en las que el tiempo de conducción continua del titular de la tarjeta llega a un múltiplo de tres horas,

— posición del vehículo,

— La exactitud del GNSS, fecha y hora en que se haya determinado la posición.

306) La tarjeta de conductor deberá ser capaz de almacenar al menos 252 de estos registros.

4.5.4 *Tarjeta de taller*

4.5.4.1 Aplicación del tacógrafo (accesible a las unidades instaladas en vehículos de primera y segunda generación)

4.5.4.1.1 Identificación de la aplicación

307) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos de identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

4.5.4.1.2 Claves y certificados

308) La tarjeta de taller deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte A.

309) La tarjeta de taller deberá ser capaz de almacenar un número de identificación personal (código PIN).

4.5.4.1.3 Identificación de la tarjeta

310) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidieron la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de expiración de la tarjeta.

4.5.4.1.4 Identificación del titular de la tarjeta

311) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre del taller,

— dirección del taller,

— apellido(s) del titular,

— nombre(s) del titular,

— idioma preferido.

4.5.4.1.5 Transferencia de los datos de la tarjeta

312) La tarjeta de taller deberá ser capaz de almacenar un registro de datos sobre transferencias de la tarjeta, del mismo modo que una tarjeta de conductor.

4.5.4.1.6 Datos de calibrado y de ajuste de la hora

313) La tarjeta de taller deberá ser capaz de mantener almacenados los registros de los calibrados o ajustes de hora que se hayan realizado mientras la tarjeta está insertada en el aparato de control.

314) Cada registro de calibrado deberá ser capaz de mantener almacenados los datos siguientes:

— propósito del calibrado (activación, primera instalación, instalación, control periódico),

— identificación del vehículo,

— parámetros que se actualizan o confirman (w, k, l, tamaño de los neumáticos, valor de ajuste del dispositivo limitador de la velocidad, cuentakilómetros (lectura anterior y nueva lectura), fecha y hora (valor anterior y nuevo valor),

— identificación del aparato de control (número de pieza de la VU, número de serie de la VU, número de serie del sensor de movimiento).

315) La tarjeta de taller deberá ser capaz de almacenar al menos 88 de estos registros.

316) La tarjeta de taller deberá tener un contador que indique el número total de calibrados que se hayan realizado con la tarjeta.

317) La tarjeta de taller deberá tener un contador que indique el número de calibrados que se hayan realizado desde la última transferencia.

4.5.4.1.7 Datos de incidentes y fallos

318) La tarjeta de taller deberá ser capaz de almacenar los registros de datos sobre fallos e incidentes, del mismo modo que una tarjeta de conductor.

319) La tarjeta de taller deberá ser capaz de almacenar los datos de los tres incidentes más recientes de cada tipo (es decir, dieciocho incidentes) y de los seis fallos más recientes de cada tipo (es decir, doce fallos).

4.5.4.1.8 Datos sobre la actividad del conductor

320) La tarjeta de taller deberá ser capaz de almacenar datos sobre la actividad del conductor, del mismo modo que una tarjeta de conductor.

321) La tarjeta de taller deberá ser capaz de mantener almacenados los datos sobre la actividad del conductor durante al menos un día de actividad media.

4.5.4.1.9 Datos sobre vehículos empleados

322) La tarjeta de taller deberá ser capaz de almacenar registros de datos sobre los vehículos empleados, del mismo modo que una tarjeta de conductor.

323) La tarjeta de taller deberá ser capaz de almacenar al menos cuatro de estos registros.

4.5.4.1.10 Datos sobre el comienzo y el final de los períodos de trabajo diarios

324) La tarjeta de taller deberá ser capaz de almacenar los registros de datos sobre las horas de comienzo o final de los períodos de trabajo diarios, del mismo modo que una tarjeta de conductor.

325) La tarjeta de taller deberá ser capaz de mantener almacenados al menos tres pares de estos registros.

4.5.4.1.11 Datos de la sesión

326) La tarjeta de taller deberá ser capaz de almacenar un registro de datos de sesión, del mismo modo que una tarjeta de conductor.

4.5.4.1.12 Datos sobre actividades de control

327) La tarjeta de taller deberá ser capaz de almacenar un registro de datos sobre actividades de control, del mismo modo que una tarjeta de conductor.

4.5.4.1.13 Datos sobre condiciones específicas

328) La tarjeta de taller deberá ser capaz de almacenar los datos correspondientes a las condiciones específicas, del mismo modo que la tarjeta de conductor.

329) La tarjeta de taller deberá ser capaz de almacenar al menos dos de estos registros.

4.5.4.2 Aplicación de tacógrafo de segunda generación (no accesible a la unidad instalada en el vehículo de primera generación)

4.5.4.2.1 Identificación de la aplicación

330) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos de identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

4.5.4.2.2 Claves y certificados

331) La tarjeta de taller deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte B.

332) La tarjeta de taller deberá ser capaz de almacenar un número de identificación personal (código PIN).

4.5.4.2.3 Identificación de la tarjeta

333) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidieron la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de expiración de la tarjeta.

4.5.4.2.4 Identificación del titular de la tarjeta

334) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre del taller,

— dirección del taller,

— apellido(s) del titular,

— nombre(s) del titular,

— idioma preferido.

4.5.4.2.5 Transferencia de los datos de la tarjeta

335) La tarjeta de taller deberá ser capaz de almacenar un registro de datos sobre transferencias de la tarjeta, del mismo modo que una tarjeta de conductor.

4.5.4.2.6 Datos de calibrado y de ajuste de la hora

336) La tarjeta de taller deberá ser capaz de mantener almacenados los registros de los calibrados o ajustes de hora que se hayan realizado mientras la tarjeta está insertada en el aparato de control.

337) Cada registro de calibrado deberá ser capaz de mantener almacenados los datos siguientes:

— propósito del calibrado (activación, primera instalación, instalación, control periódico),

— identificación del vehículo,

— parámetros que se actualizan o confirman (w, k, l, tamaño de los neumáticos, valor de ajuste del dispositivo limitador de la velocidad, cuentakilómetros (lectura anterior y nueva lectura), fecha y hora (valor anterior y nuevo valor),

— identificación del aparato de control (número de pieza de la VU, número de serie de la VU, número de serie del sensor de movimiento, número de serie del dispositivo de comunicación a distancia y número de serie del dispositivo GNSS externo, si procede),

— tipo e identificador de todos los precintos existentes,

— capacidad de la VU para utilizar tarjetas de tacógrafo de la primera generación (habilitada o no).

338) La tarjeta de taller deberá ser capaz de almacenar al menos 88 de estos registros.

339) La tarjeta de taller deberá tener un contador que indique el número total de calibrados que se hayan realizado con la tarjeta.

340) La tarjeta de taller deberá tener un contador que indique el número de calibrados que se hayan realizado desde la última transferencia.

4.5.4.2.7 Datos de incidentes y fallos

341) La tarjeta de taller deberá ser capaz de almacenar los registros de datos sobre fallos e incidentes, del mismo modo que una tarjeta de conductor.

342) La tarjeta de taller deberá ser capaz de almacenar los datos de los tres incidentes más recientes de cada tipo (es decir, treinta y tres incidentes) y de los seis fallos más recientes de cada tipo (es decir, doce fallos).

4.5.4.2.8 Datos sobre la actividad del conductor

343) La tarjeta de taller deberá ser capaz de almacenar datos sobre la actividad del conductor, del mismo modo que una tarjeta de conductor.

344) La tarjeta de taller deberá ser capaz de mantener almacenados los datos sobre la actividad del conductor durante al menos un día de actividad media.

4.5.4.2.9 Datos sobre vehículos empleados

345) La tarjeta de taller deberá ser capaz de almacenar registros de datos sobre los vehículos empleados, del mismo modo que una tarjeta de conductor.

346) La tarjeta de taller deberá ser capaz de almacenar al menos cuatro de estos registros.

4.5.4.2.10 Datos sobre el comienzo y el final de los períodos de trabajo diarios

347) La tarjeta de taller deberá ser capaz de almacenar los registros de datos sobre las horas de comienzo o final de los períodos de trabajo diarios, del mismo modo que una tarjeta de conductor.

348) La tarjeta de taller deberá ser capaz de mantener almacenados al menos tres pares de estos registros.

4.5.4.2.11 Datos de la sesión

349) La tarjeta de taller deberá ser capaz de almacenar un registro de datos de sesión, del mismo modo que una tarjeta de conductor.

4.5.4.2.12 Datos sobre actividades de control

350) La tarjeta de taller deberá ser capaz de almacenar un registro de datos sobre actividades de control, del mismo modo que una tarjeta de conductor.

4.5.4.2.13 Datos utilizados en unidades instaladas en vehículos

351) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos relativos a las diferentes unidades instaladas en vehículos en que se utilice la tarjeta:

— fecha y la hora en que comienza el período de uso de la unidad instalada en el vehículo (es decir, primera inserción de la tarjeta en la unidad instalada en el vehículo en el período),

— nombre del fabricante de la unidad instalada en el vehículo,

— tipo de unidad instalada en el vehículo,

— versión del *software* que lleva instalado la unidad instalada en el vehículo.

352) La tarjeta de taller deberá ser capaz de almacenar al menos cuatro de estos registros.

4.5.4.2.14 Datos sobre lugares en tres horas de conducción continua

353) La tarjeta de taller deberá ser capaz de almacenar los siguientes datos relativos a la posición del vehículo cuando el tiempo de conducción continua del conductor alcance un múltiplo de tres horas:

— fecha y hora en las que el tiempo de conducción continua del titular de la tarjeta llega a un múltiplo de tres horas,

— posición del vehículo,

— La exactitud del GNSS, fecha y hora en que se haya determinado la posición.

354) La tarjeta de taller deberá ser capaz de almacenar al menos dieciocho de estos registros.

4.5.4.2.15 Datos sobre condiciones específicas

355) La tarjeta de taller deberá ser capaz de almacenar los datos correspondientes a las condiciones específicas, del mismo modo que la tarjeta de conductor.

356) La tarjeta de taller deberá ser capaz de almacenar al menos dos de estos registros.

4.5.5 *Tarjeta de control*

4.5.5.1 Aplicación del tacógrafo (accesible a las unidades instaladas en vehículos de primera y segunda generación)

4.5.5.1.1 Identificación de la aplicación

357) La tarjeta de control deberá ser capaz de almacenar los siguientes datos de identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

4.5.5.1.2 Claves y certificados

358) La tarjeta de control deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte A.

4.5.5.1.3 Identificación de la tarjeta

359) La tarjeta de control deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidieron la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de expiración de la tarjeta (en su caso).

4.5.5.1.4 Identificación del titular de la tarjeta

360) La tarjeta de control deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre del organismo de control,

— dirección del organismo de control,

— apellido(s) del titular,

— nombre(s) del titular,

— idioma preferido.

4.5.5.1.5 Datos sobre actividades de control

361) La tarjeta de control deberá ser capaz de almacenar los siguientes datos sobre actividades de control:

— fecha y hora del control,

— tipo de control (visualización y/o impresión y/o transferencia de los datos de la VU y/o transferencia de los datos de la tarjeta y/o control del calibrado en carretera),

— período transferido (en su caso),

— VRN y autoridad del Estado miembro donde se matriculó el vehículo controlado,

— número de tarjeta y Estado miembro que haya expedido la tarjeta de conductor que se controla.

362) La tarjeta de control deberá ser capaz de mantener almacenados al menos 230 de estos registros.

4.5.5.2 Aplicación de tacógrafo G2 (no accesible para la unidad instalada en el vehículo de primera generación)

4.5.5.2.1 Identificación de la aplicación

363) La tarjeta de control deberá ser capaz de almacenar los siguientes datos de identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

4.5.5.2.2 Claves y certificados

364) La tarjeta de control deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte B.

4.5.5.2.3 Identificación de la tarjeta

365) La tarjeta de control deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidieron la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de expiración de la tarjeta (en su caso).

4.5.5.2.4 Identificación del titular de la tarjeta

366) La tarjeta de control deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre del organismo de control,

— dirección del organismo de control,

— apellido(s) del titular,

— nombre(s) del titular,

— idioma preferido.

4.5.5.2.5 Datos sobre actividades de control

367) La tarjeta de control deberá ser capaz de almacenar los siguientes datos sobre actividades de control:

— fecha y hora del control,

— tipo de control (visualización y/o impresión y/o transferencia de los datos de la VU y/o transferencia de los datos de la tarjeta y/o control del calibrado en carretera),

— período transferido (en su caso),

— VRN y autoridad del Estado miembro donde se matriculó el vehículo controlado,

— número de tarjeta y Estado miembro que haya expedido la tarjeta de conductor que se controla.

368) La tarjeta de control deberá ser capaz de mantener almacenados al menos 230 de estos registros.

4.5.6 *Tarjeta de empresa*

4.5.6.1 Aplicación del tacógrafo (accesible a las unidades instaladas en vehículos de primera y segunda generación)

4.5.6.1.1 Identificación de la aplicación

369) La tarjeta de empresa deberá ser capaz de almacenar los siguientes datos de identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

4.5.6.1.2 Claves y certificados

370) La tarjeta de empresa deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte A.

4.5.6.1.3 Identificación de la tarjeta

371) La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidieron la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de expiración de la tarjeta (en su caso).

4.5.6.1.4 Identificación del titular de la tarjeta

372) La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre de la empresa,

— dirección de la empresa.

4.5.6.1.5 Datos sobre la actividad de la empresa

373) La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos sobre la actividad de la empresa:

— fecha y hora de la actividad,

— tipo de actividad (activación o desactivación del bloqueo de la VU, o transferencia de los datos de la VU o transferencia de los datos de la tarjeta),

— período transferido (en su caso),

— VRN y autoridad del Estado miembro donde se matriculó el vehículo,

— número de tarjeta y Estado miembro que haya expedido la tarjeta (en caso de transferencia de los datos de la tarjeta).

374) La tarjeta de la empresa deberá ser capaz de mantener almacenados al menos 230 de estos registros.

4.5.6.2 Aplicación de tacógrafo G2 (no accesible para la unidad instalada en el vehículo de primera generación)

4.5.6.2.1 Identificación de la aplicación

375) La tarjeta de empresa deberá ser capaz de almacenar los siguientes datos de identificación de la aplicación:

— identificación de la aplicación del tacógrafo,

— identificación del tipo de tarjeta de tacógrafo.

4.5.6.2.2 Claves y certificados

376) La tarjeta de empresa deberá ser capaz de almacenar una serie de claves y certificados criptográficos, según lo especificado en el apéndice 11, parte B.

4.5.6.2.3 Identificación de la tarjeta

377) La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos relativos a la identificación de la tarjeta:

— número de tarjeta,

— nombre del Estado miembro y de la autoridad que expidieron la tarjeta, fecha de expedición,

— fecha de comienzo de validez de la tarjeta, fecha de expiración de la tarjeta (en su caso).

4.5.6.2.4 Identificación del titular de la tarjeta

378) La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos relativos a la identificación del titular de la tarjeta:

— nombre de la empresa,

— dirección de la empresa.

4.5.6.2.5 Datos sobre la actividad de la empresa

379) La tarjeta de la empresa deberá ser capaz de almacenar los siguientes datos sobre la actividad de la empresa:

— fecha y hora de la actividad,

— tipo de actividad (activación o desactivación del bloqueo de la VU, o transferencia de los datos de la VU o transferencia de los datos de la tarjeta),

— período transferido (en su caso),

— VRN y autoridad del Estado miembro donde se matriculó el vehículo,

— número de tarjeta y Estado miembro que haya expedido la tarjeta (en caso de transferencia de los datos de la tarjeta).

380) La tarjeta de la empresa deberá ser capaz de mantener almacenados al menos 230 de estos registros.

5 INSTALACIÓN DEL APARATO DE CONTROL

5.1 **Instalación**

381) El aparato de control nuevo deberá entregarse desactivado al instalador o al fabricante del vehículo, con todos los parámetros de calibrado que se relacionan en el capítulo 3.21 configurados según sus valores válidos por defecto. Si no existe un valor en particular que deba considerarse adecuado por defecto, los parámetros literales deberán configurarse con cadenas de interrogantes («?») y los valores numéricos deberán ajustarse a cero («0»). La entrega de piezas del aparato de control importantes para la seguridad podrá limitarse, si fuera necesario, durante la certificación de seguridad.

382) Antes de ser activado, el aparato de control tendrá que dar acceso a la función de calibrado, aunque no se encuentre en el modo de calibrado.

383) Antes de ser activado, el aparato de control no deberá registrar ni almacenar los datos mencionados en los puntos 3.12.3, 3.12.9 y 3.12.12 a 3.12.15 inclusive.

384) Durante la instalación, el fabricante del vehículo deberá preconfigurar todos los parámetros conocidos.

385) Los fabricantes de vehículos o los instaladores deberán activar el aparato de control instalado como máximo antes de que el vehículo se utilice con arreglo al Reglamento (CE) n.º 561/2006.

386) El aparato de control se activará automáticamente al insertar por primera vez una tarjeta de taller válida en cualquiera de sus dispositivos de interfaz para tarjetas.

387) Las operaciones específicas de emparejamiento que se precisan entre el sensor de movimiento y la unidad instalada en el vehículo, si las hay, deberán producirse automáticamente antes o durante la activación.

388) De forma semejante, las operaciones específicas de acoplamiento entre el dispositivo GNSS externo y la unidad instalada en el vehículo, si las hay, deberán producirse automáticamente antes o durante la activación.

389) Una vez activado, el aparato de control deberá permitir el uso de todas las funciones y derechos de acceso a los datos.

390) Una vez activado, el aparato de control deberá comunicar al dispositivo de comunicación a distancia los datos seguros necesarios a efectos de los controles en carretera selectivos.

391) Una vez activado el aparato de control, las funciones de registro y almacenamiento serán totalmente operativas.

392) Tras la instalación, deberá efectuarse un calibrado. El primer calibrado podrá no incluir necesariamente la introducción del número de matrícula del vehículo (VRN) si el taller autorizado encargado de realizar el calibrado no lo conoce. En estas circunstancias, el propietario del vehículo podrá introducir, tan solo por esta vez, el VRN utilizando su tarjeta de empresa antes de destinar el vehículo a los usos consentidos por el Reglamento (CE) n.º 561/2006 (por ejemplo, utilizando comandos mediante una estructura de menú apropiada de la interfaz persona-máquina de la unidad instalada en el vehículo) ([1]). Para actualizar o confirmar los datos introducidos deberá utilizarse, necesariamente, una tarjeta de taller.

393) La instalación de un dispositivo GNSS externo requiere el acoplamiento con la unidad instalada en el vehículo y la subsiguiente verificación de la información de posición del GNSS.

394) El aparato de control deberá colocarse en el vehículo de modo que el conductor pueda acceder a las funciones necesarias desde su asiento.

([1]) DO L 102, 11.4.2006, p.1

5.2 **Placa de instalación**

395) Después de haber instalado y verificado el aparato de control, se le fijará una placa de instalación, grabada o impresa de forma permanente, que sea bien visible y de fácil acceso. Cuando esto no sea posible, la placa se fijará en el montante «B» del vehículo para que sea claramente visible. En aquellos vehículos sin montante «B», la placa se fijará en el marco de la puerta del lado del conductor del vehículo y deberá quedar a la vista en cualquier caso.

Después de cada nueva inspección por un taller o instalador autorizado, la placa deberá sustituirse por otra nueva.

396) En la placa deberán figurar, como mínimo, los datos siguientes:

— nombre y domicilio o nombre comercial del instalador o taller autorizado,

— coeficiente característico del vehículo, en la forma «w = … imp/km»,

— constante del aparato de control, en la forma «k = … imp/km»,

— circunferencia efectiva de los neumáticos de las ruedas, en la forma «l = … mm»,

— tamaño de los neumáticos,

— fecha del informe del coeficiente característico del vehículo y de la medida de la circunferencia efectiva de los neumáticos de las ruedas,

— número de identificación del vehículo (VIN),

— presencia (o no) de un dispositivo GNSS externo,

— número de serie del dispositivo GNSS externo,

— número de serie del dispositivo de comunicación a distancia,

— número de serie de todos los precintos existentes.

— parte del vehículo en la que, en su caso, está instalado el adaptador,

— parte del vehículo en la que está instalado el sensor de movimiento, si no está conectado a la caja de cambios o si no se utiliza un adaptador,

— descripción del color del cable entre el adaptador y la parte del vehículo que proporciona sus impulsos de entrada,

— número de serie del sensor de movimiento integrado del adaptador.

397) Únicamente en los vehículos de las categorías M1 y N1, equipados con un adaptador conforme a las disposiciones del Reglamento (CE) n.º 68/2009 de la Comisión ([1]) en su versión modificada más reciente, y cuando no se pueda incluir toda la información necesaria según el requisito 396, se podrá utilizar una segunda placa adicional. En estos casos, esta placa adicional contendrá, al menos, la información descrita en los últimos cuatro guiones del requisito 396.

De instalar esta segunda placa adicional, se colocará junto a la primera placa principal descrita en el requisito 396 o cerca de ella, y se aplicará el mismo nivel de protección. Asimismo, la segunda placa deberá indicar el nombre, dirección o denominación comercial del instalador o taller que haya efectuado la instalación, junto con la fecha de instalación

([1]) Reglamento (CE) n.o 68/2009 de la Comisión, de 23 de enero de 2009, por el que se adapta por novena vez al progreso técnico el Reglamento (CEE) n.o 3821/85 del Consejo relativo al aparato de control en el sector de los transportes por carretera (DO L 21 de 24.1.2009, p. 3).

5.3 **Precintos**

398) Deberán precintarse los elementos siguientes:

— cualquier conexión que, de estar desconectada, ocasionaría modificaciones o pérdidas de datos indetectables (esto puede aplicarse, por ejemplo, a la instalación del sensor de movimiento en la caja de cambios, al adaptador para vehículos M1/N1, a la conexión del GNSS externo o la unidad instalada en el vehículo),

— la placa de instalación, salvo que esté sujeta de tal modo que no pueda retirarse sin destruir las inscripciones que figuran en ella.

399) Los precintos anteriormente mencionados podrán quitarse:

— en caso de urgencia,

— para instalar, ajustar o reparar un dispositivo de limitación de velocidad o cualquier otro dispositivo que contribuya a la seguridad vial, siempre que el aparato de control siga funcionando de forma fiable y correcta y vuelva a ser precintado por un instalador o taller autorizado (de acuerdo con lo dispuesto en el capítulo 6) inmediatamente después de que se haya instalado el dispositivo de limitación de velocidad o cualquier otro dispositivo que contribuya a la seguridad vial, o en el plazo de siete días en otros casos.

400) Siempre que se retiren estos precintos deberá redactarse y ponerse a disposición de la autoridad competente una justificación de esta medida.

401) Los precintos deberán llevar un número de identificación, asignado por su fabricante. Este número deberá ser único y distinto de cualquier otro número de precinto asignado por otro fabricante de precintos.

Este número de identificación único se define del siguiente modo: MM NNNNNN mediante marcado que no se pueda retirar, siendo MM un identificador único del fabricante (registro en base de datos gestionada por la CE) y NNNNNN identificador alfanumérico del precinto, único en el dominio del fabricante.

402) Los precintos dispondrán de un espacio libre en el que instaladores, talleres o fabricantes de vehículos puedan añadir una marca especial con arreglo al artículo 22, apartado 3, del Reglamento (UE) n.º 165/2014.

Esta marca no deberá tapar el número de identificación del precinto.

403) Los fabricantes de los precintos quedarán registrados en una base de datos específica y hará públicos sus identificadores de precintos a través de un procedimiento que establecerá la Comisión Europea.

404) Los talleres autorizados y los fabricantes de vehículos utilizarán únicamente, en el marco del Reglamento (UE) n.º 165/2014, precintos procedentes de los fabricantes de precintos recogidos en la base de datos mencionada anteriormente.

405) Los fabricantes de precintos y sus distribuidores mantendrán registros de trazabilidad completa de los precintos vendidos para su uso en el marco del Reglamento (UE) n.º 165/2014, que podrán mostrar a las autoridades nacionales competentes cuando sea necesario.

406) Los identificadores únicos de los precintos deberán ser visible en la placa de instalación.

6 VERIFICACIONES, CONTROLES Y REPARACIONES

En el capítulo 5.3 del presente anexo se definen las circunstancias en las que podrán quitarse los precintos, según lo indicado en el artículo 22, apartado 5, del Reglamento (UE) n.º 165/2014.

6.1 **Autorización de instaladores, talleres y fabricantes de vehículos**

Los Estados miembros aprobarán, inspeccionarán periódicamente y certificarán los organismos encargados de realizar:

— instalaciones,

— verificaciones,

— controles,

— reparaciones.

Las tarjetas de taller se expedirán únicamente a los instaladores o talleres que hayan sido autorizados para proceder a la activación o calibrado del aparato de control de conformidad con el presente anexo y que además, salvo justificación:

— no puedan optar a recibir una tarjeta de empresa,

— sus demás actividades profesionales no supongan un compromiso potencial de la seguridad general del sistema tal y como se exige en el apéndice 10.

6.2 **Verificación de instrumentos nuevos o reparados**

407) Cada dispositivo, tanto nuevo como reparado, deberá verificarse individualmente en lo que se refiere a su correcto funcionamiento y a la exactitud de sus indicaciones y registros, dentro de los límites establecidos en los capítulos 3.2.1, 3.2.2, 3.2.3 y 3.3, mediante la colocación de un precinto, de acuerdo con lo dispuesto en el capítulo 5.3, y la realización de un calibrado.

6.3 **Control de la instalación**

408) En el momento de su instalación en un vehículo, la instalación en su conjunto (incluido el aparato de control) deberá ajustarse a las disposiciones sobre tolerancias máximas establecidas en los capítulos 3.2.1, 3.2.2, 3.2.3 y 3.3.

6.4 **Controles periódicos**

409) Los aparatos instalados en los vehículos se someterán a un control periódico cada vez que se repare el aparato o se efectúe cualquier modificación del coeficiente característico del vehículo o de la circunferencia efectiva de los neumáticos de las ruedas, o si la hora UTC del aparato presenta un retraso o un adelanto de más de 20 minutos, o si cambia el VRN, o al menos en el plazo de dos años (24 meses) desde el último control.

410) Se controlará, en particular:

— que el aparato de control ejecute correctamente todas sus funciones, incluidas la función de almacenamiento de datos en las tarjetas de tacógrafo y la comunicación con los lectores de comunicación a distancia,

— que se cumpla lo dispuesto en los capítulos 3.2.1 y 3.2.2 sobre tolerancias máximas al realizarse la instalación,

— que se cumpla lo dispuesto en los capítulos 3.2.3 y 3.3,

— que el aparato de control lleve la marca de homologación,

— que se coloquen una placa de instalación, según la define el requisito 396, y una placa descriptiva, según la define el requisito 225,

— el tamaño de los neumáticos y la circunferencia real de los neumáticos.

— que no haya dispositivos de manipulación integrados en el aparato,

— que los precintos estén correctamente colocados, en buen estado, que sus identificadores sean válidos (fabricante del precinto incluido en la base de datos de la CE) y que sus identificadores correspondan a las marcas de la placa de instalación (véase el requisito 401).

411) Si se comprueba que se ha producido alguno de los incidentes enumerados en el capítulo 3.9 («Detección de incidentes y/o fallos») desde el último control y los fabricantes del tacógrafo y/o las autoridades nacionales lo consideran potencialmente peligroso para la seguridad del aparato, el taller deberá:

a. comparar los datos de identificación del sensor de movimiento conectado a la caja de cambios con los del sensor de movimiento acoplado registrados en la unidad instalada en el vehículo;

b. comprobar si la información registrada en la placa de instalación se corresponde con la registrada en la unidad instalada en el vehículo;

c. verificar si los números de serie y homologación del sensor de movimiento, si están impresos en la carcasa de este último, casan con la información almacenada en la memoria de datos del aparato de control;

d. comparar los datos de identificación marcados en la placa descriptiva del dispositivo GNSS externo, si existe, con los almacenados en la memoria de datos de la unidad instalada en el vehículo.

412) Los talleres consignaran en sus informes de control cualquier conclusión relativa a la existencia de precintos rotos o de dispositivos de manipulación. Los talleres deberán conservar dichos informes durante al menos dos años y los pondrán a disposición de la autoridad competente cuando se les solicite.

413) Estos controles incluirán un calibrado y una sustitución preventiva de los precintos cuya instalación está bajo la responsabilidad de los talleres.

6.5 **Determinación de errores**

414) La determinación de los errores de instalación y de uso deberá efectuarse en las condiciones siguientes, que se considerarán condiciones normales de ensayo:

— vehículo vacío, en condiciones normales de marcha,

— presión de los neumáticos conforme a las instrucciones del fabricante,

— desgaste de los neumáticos dentro de los límites admitidos por las normas nacionales en vigor,

— movimiento del vehículo:

— este deberá desplazarse, movido por su propio motor, en línea recta por una superficie plana a una velocidad de 50 ± 5 km/h; la distancia de medición será de al menos 1 000 m,

— el ensayo podrá realizarse también en un banco de pruebas adecuado o con otros métodos, si garantizan una precisión similar.

6.6 **Reparaciones**

415) Los talleres deberán ser capaces de extraer los datos del aparato de control para facilitarlos a la empresa de transportes que corresponda.

416) Los talleres autorizados deberán expedir a las empresas de transportes un certificado de intransferibilidad de los datos cuando un fallo en el funcionamiento del aparato impida transferir los datos previamente registrados, incluso después de una reparación por el taller en cuestión. Los talleres conservarán en su poder durante al menos dos años una copia de cada certificado expedido.

7 EXPEDICIÓN DE TARJETAS

Los procedimientos de expedición de tarjetas que establezcan los Estados miembros deberán cumplir las condiciones siguientes:

417) En el número de la primera tarjeta de tacógrafo expedida para un solicitante, el índice consecutivo (en su caso), el índice de sustitución y el índice de renovación serán «0».

418) Los números de todas las tarjetas de tacógrafo no personales que se expidan a un mismo organismo de control, taller o empresa de transportes empezarán por los mismos 13 dígitos, y todos ellos tendrán un índice consecutivo diferente.

419) Cuando se expida una tarjeta de tacógrafo en sustitución de otra ya existente, la nueva llevará el mismo número de tarjeta que la sustituida, con excepción del índice de sustitución, que se verá incrementado en una unidad (en el orden 0, …, 9, A, …, Z).

420) Cuando se expida una tarjeta de tacógrafo en sustitución de otra ya existente, la nueva tendrá la misma fecha de expiración que la sustituida.

421) Cuando se expida una tarjeta de tacógrafo para renovar otra ya existente, la nueva llevará el mismo número de tarjeta que la sustituida, con excepción del índice de sustitución, que se pondrá a «0», y el índice de renovación, que se verá incrementado en una unidad (en el orden 0, …, 9, A, …, Z).

422) Cuando se sustituya una tarjeta de tacógrafo existente para modificar datos administrativos, se observarán las reglas de renovación si el cambio se efectúa en el mismo Estado miembro, o las reglas de primera expedición si el cambio lo efectúa otro Estado miembro.

423) La rúbrica «apellidos del titular de la tarjeta» de las tarjetas de control o de taller que no sean personales indicará el nombre del taller o del organismo de control, o el nombre del instalador o del controlador si el Estado miembro así lo decide.

424) Los Estados miembros intercambiarán datos por vía electrónica a fin de garantizar la unicidad de las tarjetas de conductor que expiden, de conformidad con el artículo 31 del Reglamento (UE) n.º 165/2014.

8 HOMOLOGACIÓN DEL APARATO DE CONTROL Y DE LAS TARJETAS DE TACÓGRAFO

8.1 **Generalidades**

A efectos del presente capítulo, por «aparato de control» se entenderá el «aparato de control o sus componentes». No será preciso homologar el cable o cables que conectan el sensor de movimiento a la VU, el dispositivo GNSS externo a la VU o el dispositivo de comunicación a distancia a la VU. El papel que utilice el aparato de control se considerará un componente de dicho aparato.

Todo fabricante podrá solicitar la homologación de su componente con cualquier tipo de sensor de movimiento, dispositivo GNSS externo y viceversa, siempre que cada componente cumpla los requisitos del presente anexo. De manera alternativa, los fabricantes podrán también solicitar la homologación del aparato de control.

425) El aparato de control deberá presentarse a la homologación provisto de los eventuales dispositivos complementarios integrados.

426) La homologación del aparato de control y de las tarjetas de tacógrafo deberá incluir ensayos relacionados con la seguridad, ensayos funcionales y ensayos de interoperabilidad. El resultado positivo de cada uno de estos ensayos se consignará en un certificado.

427) Las autoridades de homologación de los Estados miembros no concederán el certificado de homologación si no están en posesión de:

— un certificado de seguridad,

— un certificado funcional, y

— un certificado de interoperabilidad

para el aparato de control o la tarjeta de tacógrafo cuya homologación se solicite.

428) Todo cambio que se introduzca en el *software* o el *hardware* del aparato de control o en la naturaleza de los materiales empleados en su fabricación deberá notificarse, antes de su utilización, a la autoridad que haya homologado el aparato. Dicha autoridad deberá confirmar al fabricante la ampliación de la homologación, o bien podrá exigir una actualización o confirmación del certificado funcional, de seguridad o de interoperabilidad.

429) Los procesos de actualización *in situ* del *software* empleado por el aparato de control precisarán la aprobación de la autoridad que haya homologado el aparato. La actualización del *software* no deberá alterar ni borrar los datos sobre la actividad del conductor que haya almacenados en el aparato de control. El *software* sólo podrá actualizarse bajo la responsabilidad del fabricante del aparato.

430) No podrá denegarse la homologación de las modificaciones del *software* destinadas a la mejora de un aparato de control previamente homologado si tales modificaciones solo se aplican a funciones no especificadas en el presente anexo. La actualización del *software* de un aparato de control podrá excluir la introducción de juegos de caracteres nuevos, si no es técnicamente viable.

8.2 **Certificado de seguridad**

431) El certificado de seguridad se entrega según lo dispuesto en el apéndice 10 del presente anexo. Los componentes del aparato de control que se han de certificar son la unidad instalada en el vehículo, el sensor de movimiento, el dispositivo GNSS externo y las tarjetas de tacógrafo.

432) En el caso excepcional de que las autoridades de certificación de la seguridad se nieguen a certificar un nuevo aparato basándose en la obsolescencia de los mecanismos de seguridad, la homologación seguirá concediéndose única y exclusivamente en estas circunstancias específicas y excepcionales, y siempre que no exista una solución alternativa que se ajuste al Reglamento.

433) En esta circunstancia, el Estado miembro interesado informará sin dilación a la Comisión Europea, que iniciará, en un plazo de doce meses civiles desde la concesión de la homologación, un procedimiento que garantice el restablecimiento del nivel de seguridad a sus niveles originales.

8.3 **Certificado funcional**

434) Cada candidato a recibir una homologación deberá facilitar a la autoridad de homologación del Estado miembro que corresponda todo el material y la documentación que dicha autoridad estime necesario.

435) Los fabricantes deberán aportar las muestras oportunas de los productos candidatos a la homologación y la documentación asociada solicitada por los laboratorios encargados de realizar los ensayos funcionales en el plazo de un mes desde que se formule dicha solicitud. Todos los costes derivados de dicha solicitud correrán a cargo de la entidad solicitante. Los laboratorios preservarán la confidencialidad de todos los datos comercialmente sensibles.

436) El certificado funcional deberá entregarse al fabricante solo después de haberse superado como mínimo todos los ensayos funcionales especificados en el apéndice 9.

437) El certificado funcional lo entrega la autoridad de homologación. Dicho certificado deberá incluir, además del nombre de su beneficiario y la identificación del modelo, una relación pormenorizada de los ensayos que se hayan realizado, junto con los resultados obtenidos.

438) El certificado funcional de un componente del aparato de control deberá indicar, asimismo, los números de homologación de los demás componentes compatibles del aparato de control homologados sometidos a ensayo para su certificación.

439) El certificado funcional de un componente del aparato de control deberá indicar, asimismo, la norma ISO o CEN con arreglo a la cual se haya certificado la interfaz funcional.

8.4 **Certificado de interoperabilidad**

440) Los ensayos de interoperabilidad las lleva a cabo un único laboratorio bajo la autoridad y la responsabilidad de la Comisión Europea.

441) Dicho laboratorio deberá registrar en el orden cronológico de recepción las solicitudes de ensayo que presenten los fabricantes.

442) Las solicitudes sólo se registrarán oficialmente cuando el laboratorio esté en posesión de:

— todo el material y los documentos necesarios para dichos ensayos de interoperabilidad,

— el correspondiente certificado de seguridad,

— el correspondiente certificado funcional.

La fecha de registro de la solicitud deberá notificarse al fabricante.

443) El laboratorio no realizará ensayos de interoperabilidad con aparatos de control o tarjetas de tacógrafo que no hayan obtenido un certificado de seguridad y un certificado funcional, salvo en las circunstancias excepcionales descritas en el requisito 432.

444) Todo el material y los documentos facilitados por el fabricante que solicite ensayos de interoperabilidad quedarán en manos del laboratorio encargado de dichos ensayos.

445) Los ensayos de interoperabilidad deberán llevarse a cabo con arreglo a lo dispuesto en el apéndice 9 del presente anexo e incluirán todos los tipos de aparatos de control o tarjetas de tacógrafo:

— que dispongan de una homologación válida, o bien

— que estén pendientes de ser homologados y dispongan de un certificado de interoperabilidad válido.

446) Los ensayos de interoperabilidad deberán cubrir todas las generaciones de aparatos de control o tarjetas de tacógrafo todavía en uso.

447) El laboratorio no entregará el certificado de interoperabilidad al fabricante hasta que se hayan superado todos los ensayos de interoperabilidad exigidos.

448) Si uno o varios aparatos de control o tarjetas de tacógrafo no superan los ensayos de interoperabilidad, el certificado de interoperabilidad no se entregará hasta que el fabricante que presente la solicitud haya realizado las modificaciones necesarias y superado dichos ensayos. El laboratorio deberá identificar la causa del problema con ayuda de los fabricantes que se vean afectados por dicho fallo de interoperabilidad, y procurará ayudar al fabricante que presente la solicitud a encontrar una solución técnica. Si el fabricante ha modificado su producto, será responsabilidad suya comprobar, mediante consulta a las autoridades pertinentes, que el certificado de seguridad y los certificados funcionales siguen siendo válidos.

449) El certificado de interoperabilidad tendrá una validez de seis meses y quedará revocado al finalizar este período si el fabricante no ha recibido el correspondiente certificado de homologación. El fabricante entrega el certificado de interoperabilidad a la autoridad de homologación del Estado miembro que ha otorgado el certificado funcional.

450) Ningún elemento que pudiera haber causado un fallo de interoperabilidad deberá utilizarse con afán de lucro o para lograr una posición dominante.

8.5 **Certificado de homologación**

451) La autoridad de homologación del Estado miembro podrá entregar el certificado de homologación del modelo en cuanto esté en posesión de los tres certificados necesarios.

452) El certificado de homologación de cualquier componente del aparato de control deberá indicar, asimismo, los números de homologación de los demás aparatos de control interoperables homologados.

453) Cuando entregue el certificado de homologación al fabricante, la autoridad de homologación deberá facilitar una copia al laboratorio encargado de los ensayos de interoperabilidad.

454) El laboratorio competente para los ensayos de interoperabilidad deberá mantener un sitio web público donde se pueda consultar una relación actualizada de los modelos de aparato de control o de tarjetas de tacógrafo:

— para los que se haya registrado una solicitud de ensayos de interoperabilidad,

— que hayan recibido un certificado de interoperabilidad (aunque sea provisional),

— que hayan recibido un certificado de homologación.

8.6 **Procedimiento de excepción: primeros certificados de interoperabilidad para los aparatos de control y las tarjetas de tacógrafo de segunda generación**

455) Hasta cuatro meses después de haberse certificado que una primera pareja de aparato de control de segunda generación y tarjetas de tacógrafo (tarjetas de conductor, de taller, de control y de empresa) de segunda generación es interoperable, se considerarán provisionales los certificados de interoperabilidad entregados (incluido los primeros) en relación con solicitudes registradas durante este período.

456) Si al finalizar este período todos los productos afectados interoperan sin problemas entre sí, los certificados de interoperabilidad correspondientes adquirirán un carácter definitivo.

457) Si durante este período se detectan fallos de interoperabilidad, el laboratorio encargado de los ensayos de interoperabilidad deberá identificar las causas de los problemas con ayuda de todos los fabricantes implicados, y les invitará a realizar las modificaciones necesarias.

458) Si al finalizar este período persisten los problemas de interoperabilidad, el laboratorio encargado de los ensayos de interoperabilidad, con la colaboración de los fabricantes implicados y con las autoridades de homologación que otorguen los correspondientes certificados funcionales, deberán determinar las causas de los fallos de interoperabilidad y establecer las modificaciones que debería introducir cada uno de los fabricantes afectados. La búsqueda de soluciones técnicas deberá prolongarse un máximo de dos meses. Si transcurre este plazo sin haberse hallado una solución común, la Comisión, previa consulta al laboratorio encargado de los ensayos de interoperabilidad, deberá decidir qué aparato(s) y tarjetas obtienen un certificado de interoperabilidad definitivo, y fundamentar su decisión.

459) Deberá posponerse hasta que se hayan resuelto los problemas de interoperabilidad iniciales cualquier solicitud de ensayos de interoperabilidad que registre el laboratorio entre el final del período de cuatro meses posterior al primer certificado de interoperabilidad provisional y la fecha en que la Comisión adopta la decisión mencionada en el requisito 455. Dichas solicitudes se procesarán luego en el orden cronológico en que se registraron.

Apéndice 1

DICCIONARIO DE DATOS

ÍNDICE

1. INTRODUCCIÓN

En el presente apéndice se especifican diversos formatos, elementos y estructuras para su uso en el aparato de control y las tarjetas de tacógrafo.

1.1. **Enfoque de la definición de los tipos de datos**

En el presente apéndice se utiliza la Notación de Sintaxis Abstracta Uno (ASN.1) para definir los tipos de datos. Ello permite definir datos simples y estructurados sin necesidad de una sintaxis específica de transferencia (reglas de codificación), que dependerá de la aplicación y del entorno.

Las convenciones sobre la denominación de los tipos ASN.1 se ajustan a la norma ISO/CEI 8824-1. Esto significa que:

— siempre que sea posible, el significado de un tipo de datos se deduce de los nombres seleccionados,

— cuando un tipo de datos se compone de otros tipos, el nombre del tipo de datos sigue siendo una secuencia única de caracteres alfabéticos que comienzan con una mayúscula, aunque las mayúsculas se utilizan en el nombre para transmitir el correspondiente significado,

— en general, los nombres de los tipos de datos están relacionados con el nombre de los tipos de datos de los que se derivan, con el equipo en que se almacenan los datos y con la función asociada a dichos datos.

Si un tipo ASN.1 ya se ha definido como parte de otra norma y es pertinente para su uso en el aparato de control, entonces ese tipo ASN.1 se definirá en el presente apéndice.

Para que pueda haber diferentes tipos de reglas de codificación, algunos tipos ASN.1 del presente apéndice están limitados por identificadores de intervalos de valores. Dichos identificadores se definen en el apartado 3 y en el apéndice 2.

1.2. **Referencias**

En el presente apéndice aparecen las siguientes referencias:

ISO 639	Código para la representación de nombres de lenguas. Primera edición: 1988.
ISO 3166	Códigos para la representación de los nombres de los países y sus subdivisiones — Parte 1: Códigos de país, 2013.
ISO 3779	Vehículos de carretera — Número de identificación del vehículo (VIN) — Contenido y estructura. 2009.
ISO/CEI 7816-5	Tarjetas de identificación — Tarjetas con circuitos integrados — Parte 5: Registro de proveedores de aplicaciones. Segunda edición: 2004.
ISO/CEI 7816-6	Tarjetas de identificación — Tarjetas con circuitos integrados — Parte 6: Elementos de datos intersectoriales para los intercambios, 2004 + Corrigendum técnico 1: 2006.
ISO/CEI 8824-1	Tecnología de la información — Notación de Sintaxis Abstracta 1 (ASN.1): Especificación de la notación básica. 2008 + Corrigendum técnico 1: 2012 y Corrigendum técnico 2: 2014.
ISO/CEI 8825-2	Tecnología de la información — Reglas de codificación ASN.1: Especificación de las Reglas de Codificación por Paquetes (PER). 2008.
ISO/CEI 8859-1	Tecnología de la información — Conjuntos de caracteres gráficos codificados con un solo byte de 8 bits — Parte 1: Alfabeto latino nº 1. Primera edición: 1998.
ISO/CEI 8859-7	Tecnología de la información — Conjuntos de caracteres gráficos codificados con un solo byte de 8 bits — Parte 7: Alfabeto latino/griego. 2003.

ISO 16844-3 Vehículos de carretera — Sistemas de tacógrafo — Interfaz del sensor de movimiento. 2004 + Corrigendum técnico 1: 2006.

TR-03110-3 BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token — Part 3 Common Specifications, version 2.20, 3. February 2015.

2. DEFINICIONES DE TIPOS DE DATOS

En todos los tipos de datos que se describen a continuación, el valor por defecto para un contenido «desconocido» o «no aplicable» consistirá en rellenar el elemento de datos con bytes 'FF'.

Todos los tipos de datos se utilizan para las aplicaciones de la generación 1 y de la generación 2, a menos que se especifique otra cosa.

2.1. **ActivityChangeInfo**

Este tipo de datos permite codificar, en una palabra de dos bytes, el estado de la ranura a las 00.00 horas y/o el estado del conductor a las 00.00 horas y/o los cambios de actividad y/o los cambios del régimen de conducción y/o los cambios del estado de la tarjeta para un conductor o un segundo conductor. Este tipo de datos está relacionado con el anexo 1C, requisitos 105, 266, 291, 320, 321, 343 y 344.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Asignación de valor — Alineación de octeto: 'scpaatttttttttt'B (16 bits)

Para registros en la memoria de datos (o estado de la ranura):

's'B Ranura:

'0'B: CONDUCTOR,

'1'B: SEGUNDO CONDUCTOR,

'c'B Régimen de conducción:

'0'B: EN SOLITARIO,

'1'B: EN EQUIPO,

'p'B Estado de la tarjeta de conductor (o de taller) en la ranura que corresponda:

'0'B: INSERTADA, hay una tarjeta insertada,

'1'B: NO INSERTADA, no hay tarjeta insertada (o se ha extraído una tarjeta),

'aa'B Actividad:

'00'B: PAUSA/DESCANSO,

'01'B: DISPONIBILIDAD,

'10'B: TRABAJO,

'11'B: CONDUCCIÓN,

'ttttttttttt'B Hora del cambio: minutos transcurridos desde las 00.00 horas de ese día.

Para registros en la tarjeta de conductor (o de taller) (y estado del conductor):

's'B	Ranura (irrelevante cuando 'p' = 1, excepto en el caso que se cita en la nota siguiente):
	'0'B: CONDUCTOR,
	'1'B: SEGUNDO CONDUCTOR,
'c'B	Régimen de conducción (caso 'p' = 0) o
	Régimen en la actividad siguiente (caso 'p' = 1):
	'0'B: EN SOLITARIO,
	'0'B: INDETERMINADO
	'1'B: EN EQUIPO,
	'1'B: DETERMINADO (= entrada manual)
'p'B	Estado de la tarjeta:
	'0'B: INSERTADA, la tarjeta está insertada en un aparato de control,
	'1'B: NO INSERTADA, la tarjeta no está insertada (o se ha extraído),
'aa'B	Actividad (irrelevante cuando 'p' = 1 y 'c' = 0, excepto en el caso citado en la nota siguiente):
	'00'B: PAUSA/DESCANSO,
	'01'B: DISPONIBILIDAD,
	'10'B: TRABAJO,
	'11'B: CONDUCCIÓN,
'ttttttttttt'B	Hora del cambio: minutos transcurridos desde las 00.00 horas de ese día.

Nota sobre el caso «extracción de la tarjeta»:

Cuando se extrae la tarjeta:

— 's' es relevante e indica la ranura de la que se extrae la tarjeta,

— 'c' debe configurarse a 0,

— 'p' debe configurarse a 1,

— 'aa' debe codificar la actividad que esté seleccionada en ese momento.

Como resultado de una entrada manual, los bits 'c' y 'aa' de la palabra (almacenada en una tarjeta) se pueden sobrescribir posteriormente para reflejar la entrada.

2.2. **Address**

Una dirección.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage especifica un conjunto de caracteres definidos en el capítulo 4.

address representa una dirección codificada utilizando el conjunto de caracteres especificado.

2.3. **AESKey**

Generación 2:

Una clave AES con una longitud de 128, 192 o 256 bits.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Asignación de valor: no hay más especificaciones.

2.4. **AES128Key**

Generación 2:

Una clave AES128.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length indica la longitud de la clave AES128 en octetos.

aes128Key es una clave AES con una longitud de 128 bits.

Asignación de valor:

La longitud deberá tener el valor 16.

2.5. **AES192Key**

Generación 2:

Una clave AES192.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length indica la longitud de la clave AES192 en octetos.

aes192Key es una clave AES con una longitud de 192 bits.

Asignación de valor:

La longitud deberá tener el valor 24.

2.6. **AES256Key**

Generación 2:

Una clave AES256.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

length indica la longitud de la clave AES256 en octetos.

aes256Key es una clave AES con una longitud de 256 bits.

Asignación de valor:

La longitud deberá tener el valor 32.

2.7. **BCDString**

La cadena BCDString se aplica para la representación decimal de codificación binaria (BCD). Este tipo de datos se utiliza para representar un dígito decimal en un semiocteto (4 bits). La cadena BCDString se basa en el 'CharacterStringType' de la norma ISO/CEI 8824-1.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

La cadena BCDString emplea una notación «hstring». El dígito hexadecimal situado más a la izquierda deberá ser el semiocteto más significativo del primer octeto. Para obtener un múltiplo de octetos habrá que insertar semioctetos nulos a la derecha, según sea necesario, a partir de la posición del semiocteto situado más a la izquierda en el primer octeto.

Los dígitos permitidos son: 0, 1, .. 9.

2.8. **CalibrationPurpose**

Código que explica por qué se registró un conjunto de parámetros de calibrado. Este tipo de datos está relacionado con el anexo 1B, requisitos 097 y 098, y con el anexo 1C, requisito 119.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Asignación de valor:

Generación 1:

'00'H	valor reservado,
'01'H	activación: registro de los parámetros de calibrado conocidos en el momento de la activación de la VU,
'02'H	primera instalación: primer calibrado de la VU después de su activación,
'03'H	instalación: primer calibrado de la VU en el vehículo actual,
'04'H	control periódico.

Generación 2:

Además de los valores de la generación 1, se utilizan los siguientes:

'05'H entrada de VRN por empresa,

'06'H ajuste de la hora sin calibrado,

'07'H a '7F'H RFU,

'80'H a 'FF'H específicos del fabricante.

2.9. CardActivityDailyRecord

Información almacenada en una tarjeta y relativa a las actividades del conductor en un día civil concreto. Este tipo de datos está relacionado con el anexo 1C, requisitos 266, 291, 320 y 343.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength es la longitud total del registro diario anterior, expresada en bytes. El valor máximo viene dado por la longitud de la CADENA DE OCTETOS que contiene dichos registros (véase CardActivityLengthRange, apéndice 2, apartado 4). Cuando este registro es el registro diario más antiguo, el valor de activityPreviousRecordLength debe configurarse a 0.

activityRecordLength es la longitud total de este registro, expresada en bytes. El valor máximo viene dado por la longitud de la CADENA DE OCTETOS que contiene dichos registros.

activityRecordDate es la fecha del registro.

activityDailyPresenceCounter es el contador de presencia diaria para esa tarjeta en ese día.

activityDayDistance es la distancia total recorrida ese día.

activityChangeInfo es el conjunto de datos de ActivityChangeInfo correspondientes al conductor en ese día. Puede contener 1 440 valores como máximo (un cambio de actividad cada minuto). Este conjunto incluye siempre la ActivityChangeInfo que codifica el estado del conductor a las 00.00 horas.

2.10. CardActivityLengthRange

Número de bytes disponibles en una tarjeta de conductor o en una tarjeta de taller para almacenar registros sobre las actividades del conductor.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Asignación de valor: véase el apéndice 2.

2.11. CardApprovalNumber

Número de homologación de la tarjeta.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Asignación de valor:

El número de homologación deberá constar según haya sido publicado en el correspondiente sitio web de la Comisión Europea, es decir, por ejemplo, incluyendo guiones si los lleva. El número de homologación deberá estar alineado a la izquierda.

2.12. **CardCertificate**

Generación 1:

Certificado de la clave pública de una tarjeta.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Información almacenada en una tarjeta y relativa a la identificación del circuito integrado (CI) de dicha tarjeta (anexo 1C, requisito 249). El icSerialNumber y el icManufacturingReferences identifican conjuntamente el chip de la tarjeta de manera única. El icSerialNumber no identifica el chip de la tarjeta de manera única por sí solo.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber es el número de serie del CI.

IcManufacturingReferences es el identificador específico del fabricante del CI.

2.14. **CardConsecutiveIndex**

El índice consecutivo de una tarjeta [definición h)].

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Asignación de valor: (véase anexo 1C, capítulo 7)

Orden de incremento: '0, …, 9, A, …, Z, a, …, z'

2.15. **CardControlActivityDataRecord**

Información almacenada en una tarjeta de conductor o de taller y relativa al último control a que ha sido sometido el conductor (anexo 1C, requisitos 274, 299, 327 y 350).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType es el tipo de control.

controlTime es la fecha y la hora del control.

controlCardNumber es el FullCardNumber del controlador que ha llevado a cabo el control.

controlVehicleRegistration es el VRN y el nombre del Estado miembro donde se matriculó el vehículo que ha sido objeto del control.

controlDownloadPeriodBegin y **controlDownloadPeriodEnd** es el período transferido, en caso de transferencia.

2.16. **CardCurrentUse**

Información acerca del uso actual de la tarjeta (anexo 1C, requisitos 273, 298, 326 y 349).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                    TimeReal,
   sessionOpenVehicle                 VehicleRegistrationIdentification
}
```

sessionOpenTime es la hora en que se inserta la tarjeta para el uso actual. Este elemento se pone a cero al extraer la tarjeta.

sessionOpenVehicle es la identificación del vehículo que se está utilizando actualmente. configurada al insertar la tarjeta. Este elemento se pone a cero al extraer la tarjeta.

2.17. **CardDriverActivity**

Información almacenada en una tarjeta de conductor o de taller y relativa a las actividades del conductor (anexo 1C, requisitos 267, 268, 292, 293, 321 y 344).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord     INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord        INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords               OCTET STRING
                                      (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord es un elemento que señala el comienzo del espacio de almacenamiento (número de bytes a partir del principio de la cadena) que corresponde al registro diario completo más antiguo en la cadena activityDailyRecords. El valor máximo viene dado por la longitud de la cadena.

activityPointerNewestRecord es un elemento que señala el comienzo del espacio de almacenamiento (número de bytes a partir del principio de la cadena) que corresponde al registro diario más reciente en la cadena activityDailyRecords. El valor máximo viene dado por la longitud de la cadena.

activityDailyRecords es el espacio disponible para almacenar los datos sobre la actividad del conductor (estructura de datos: CardActivityDailyRecord) en cada uno de los días civiles en que se ha utilizado la tarjeta.

Asignación de valor: esta cadena de octetos se va llenando cíclicamente con registros del tipo CardActivityDailyRecord. En el primer uso, el almacenamiento comienza en el primer byte de la cadena. Cada nuevo registro se añade al final del anterior. Cuando la cadena está llena, el almacenamiento continúa en el primer byte de la cadena, con independencia de si hay alguna interrupción dentro de un elemento de datos. Antes de introducir en la cadena nuevos datos de actividad (ampliando el actual activityDailyRecord, o introduciendo un nuevo activityDailyRecord) que sustituyan a datos antiguos, es preciso actualizar el activityPointerOldestDayRecord para reflejar la nueva ubicación del registro diario completo más antiguo, y además es preciso poner a 0 la longitud activityPreviousRecordLength de este (nuevo) registro diario completo más antiguo.

2.18. **CardDrivingLicenceInformation**

Información almacenada en una tarjeta de conductor y relativa a los datos correspondientes al permiso de conducir del titular de la tarjeta (anexo 1C, requisitos 259 y 284).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority es la autoridad que expidió el permiso de conducir.

drivingLicenceIssuingNation es la nacionalidad de la autoridad que expidió el permiso de conducir.

drivingLicenceNumber es el número del permiso de conducir.

2.19. **CardEventData**

Información almacenada en una tarjeta de conductor o de taller relativa a los incidentes asociados al titular de la tarjeta (anexo 1C, requisitos 260, 285, 318 y 341).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData es una secuencia de cardEventRecords ordenada por valor ascendente del código EventFaultType (excepto los registros relacionados con intentos de violación de la seguridad, que se incluyen en el último conjunto de la secuencia).

cardEventRecords es un conjunto de registros de incidentes de un tipo en particular (o de una categoría en particular, en el caso de los intentos de violación de la seguridad).

2.20. **CardEventRecord**

Información almacenada en una tarjeta de conductor o de taller y relativa a un incidente asociado al titular de la tarjeta (anexo 1C, requisitos 261, 286, 318 y 341).

```
CardEventRecord ::= SEQUENCE {
   eventType                            EventFaultType,
   eventBeginTime                       TimeReal,
   eventEndTime                         TimeReal,
   eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType es el tipo de incidente.

eventBeginTime es la fecha y la hora de comienzo del incidente.

eventEndTime es la fecha y la hora en que termina el incidente.

eventVehicleRegistration es el VRN y el nombre del Estado miembro donde se matriculó el vehículo en el que se produjo el incidente.

2.21. **CardFaultData**

Información almacenada en una tarjeta de conductor o de taller y relativa a los fallos asociados al titular de la tarjeta (anexo 1C, requisitos 263, 288, 318 y 341).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                     SET SIZE(NoOfFaultsPerType) OF
                                        CardFaultRecord
}
```

CardFaultData es una secuencia integrada por un conjunto con los registros de los fallos del aparato de control, seguido de un conjunto con los registros de los fallos de la tarjeta.

cardFaultRecords es un conjunto de registros de fallos de una categoría determinada (del aparato de control o de la tarjeta).

2.22. CardFaultRecord

Información almacenada en una tarjeta de conductor o de taller y relativa a un fallo asociado al titular de la tarjeta (anexo 1C, requisitos 264, 289, 318 y 341).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType es el tipo de fallo.

faultBeginTime es la fecha y la hora de comienzo del fallo.

faultEndTime es la fecha y la hora en que termina el fallo.

faultVehicleRegistration es el VRN y el nombre del Estado miembro donde se matriculó el vehículo en el que ocurrió el fallo.

2.23. CardIccIdentification

Información almacenada en una tarjeta y relativa a la identificación de la tarjeta con circuito integrado (CI) (anexo 1C, requisito 248).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop es el modo de parada de reloj, tal y como se define en el apéndice 2.

cardExtendedSerialNumber es el número de serie único de la tarjeta con CI, tal como se especifica más en detalle mediante el tipo de datos ExtendedSerialNumber.

cardApprovalNumber es el número de homologación de la tarjeta.

cardPersonaliserID es la identificación personal de la tarjeta codificada como ManufacturerCode.

embedderIcAssemblerId proporciona información sobre el integrador/montador del CI.

icIdentifier es el identificador del CI que incorpora la tarjeta y del fabricante de dicho CI, tal y como se define en la norma ISO/CEI 7816-6.

2.24. CardIdentification

Información almacenada en una tarjeta y relativa a la identificación de la tarjeta (anexo 1C, requisitos 255, 280, 310, 333, 359, 365, 371 y 377).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState              NationNumeric,
   cardNumber                          CardNumber,
   cardIssuingAuthorityName            Name,
   cardIssueDate                       TimeReal,
   cardValidityBegin                   TimeReal,
   cardExpiryDate                      TimeReal
}
```

cardIssuingMemberState es el código del Estado miembro que expide la tarjeta.

cardNumber es el número de la tarjeta.

cardIssuingAuthorityName es el nombre de la autoridad que ha expedido la tarjeta.

cardIssueDate es la fecha en que se expidió la tarjeta al titular actual.

cardValidityBegin es la fecha correspondiente al primer día de validez de la tarjeta.

cardExpiryDate es la fecha en que termina la validez de la tarjeta.

2.25. **CardMACertificate**

Generación 2:

Certificado de la clave pública de la tarjeta para la autenticación mutua con una VU. La estructura de este certificado se especifica en el apéndice 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Un número de tarjeta, según se indica en la definición g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification             IA5String(SIZE(14)),
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification              IA5String(SIZE(13)),
      cardConsecutiveIndex             CardConsecutiveIndex,
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   }
}
```

driverIdentification es la identificación exclusiva de un conductor en un Estado miembro.

ownerIdentification es la identificación exclusiva de una empresa, un taller o un organismo de control en un Estado miembro.

cardConsecutiveIndex es el índice consecutivo de la tarjeta.

cardReplacementIndex es el índice de sustitución de la tarjeta.

cardRenewalIndex es el índice de renovación de la tarjeta.

La primera de las dos secuencias a elegir sirve para codificar el número de una tarjeta de conductor, mientras que la segunda secuencia sirve para codificar los números de las tarjetas de taller, de control y de empresa.

2.27. **CardPlaceDailyWorkPeriod**

Información almacenada en una tarjeta de conductor o en una tarjeta de taller y relativa a los lugares donde comienzan y/o terminan los períodos de trabajo diarios (anexo 1C, requisitos 272, 297, 325 y 348).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord es el índice del último registro actualizado de un lugar.

Asignación de valor: número que corresponde al numerador del registro de un lugar. Al primer registro de la estructura se le asigna el número '0'.

placeRecords es el conjunto de registros que contienen la información relativa a los lugares introducidos.

2.28. **CardPrivateKey**

Generación 1:

La clave privada de una tarjeta.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

La clave pública de una tarjeta.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

El índice de renovación de una tarjeta [definición i)].

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Asignación de valor: (véase el capítulo VII del presente anexo).

'0' Primera expedición.

Orden de incremento: '0, …, 9, A, …, Z'

2.31. **CardReplacementIndex**

El índice de sustitución de una tarjeta [definición j)].

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Asignación de valor: (véase el capítulo VII del presente anexo).

'0' Tarjeta original.

Orden de incremento: '0, …, 9, A, …, Z'

2.32. **CardSignCertificate**

Generación 2:

Certificado de la clave pública de la tarjeta para su firma. La estructura de este certificado se especifica en el apéndice 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Código para distinguir entre las dos ranuras de una unidad instalada en el vehículo.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Asignación de valor: no hay más especificaciones.

2.34. **CardSlotsStatus**

Código que indica el tipo de tarjetas insertadas en las dos ranuras de la unidad instalada en el vehículo.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Asignación de valor — Alineación de octeto: 'ccccdddd'B

'cccc'B Identificación del tipo de tarjeta insertada en la ranura del segundo conductor,

'dddd'B Identificación del tipo de tarjeta insertada en la ranura del conductor,

con los siguientes códigos de identificación:

'0000'B no hay tarjeta insertada,

'0001'B se ha insertado una tarjeta de conductor,

'0010'B se ha insertado una tarjeta de taller,

'0011'B se ha insertado una tarjeta de control,

'0100'B se ha insertado una tarjeta de empresa.

2.35. **CardSlotsStatusRecordArray**

Generación 2:

El CardSlotsStatus más metadatos tal como se utilizan en el protocolo de transferencia.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType denota el tipo de registro (CardSlotsStatus). **Asignación de valor**: véase RecordType

recordSize es el tamaño de CardSlotsStatus en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros de CardSlotsStatus.

2.36. **CardStructureVersion**

Código que indica la versión de la estructura empleada en una tarjeta de tacógrafo.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Asignación de valor: 'aabb'H:

'aa'H Índice para cambios de la estructura,

'00'H para aplicaciones de la Generación 1

'01'H para aplicaciones de la Generación 2

'bb'H Índice para cambios relativos al uso de los elementos de datos definidos para la estructura que viene dada por el byte alto.

'00'H para esta versión de las aplicaciones de la Generación 1

'00'H para esta versión de las aplicaciones de la Generación 2

2.37. **CardVehicleRecord**

Información almacenada en una tarjeta de conductor o de taller y relativa a un período de uso de un vehículo durante un día civil (anexo 1C, requisitos 269, 294, 322 y 345).

Generación 1:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                OdometerShort,
   vehicleOdometerEnd                  OdometerShort,
   vehicleFirstUse                     TimeReal,
   vehicleLastUse                      TimeReal,
   vehicleRegistration                 VehicleRegistrationIdentification,
   vuDataBlockCounter                  VuDataBlockCounter
}
```

vehicleOdometerBegin es la lectura del cuentakilómetros del vehículo al comenzar el período de uso del vehículo.

vehicleOdometerEnd es la lectura del cuentakilómetros del vehículo al terminar el período de uso del vehículo.

vehicleFirstUse es la fecha y la hora en que comienza el período de uso del vehículo.

vehicleLastUse es la fecha y la hora en que termina el período de uso del vehículo.

vehicleRegistration es el VRN y el Estado miembro donde se ha matriculado el vehículo.

vuDataBlockCounter es el valor del VuDataBlockCounter en el momento de extraer la tarjeta por última vez en el período de uso del vehículo.

Generación 2:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Además de los de la generación 1, se utiliza el siguiente elemento de datos:

VehicleIdentificationNumber es el número de identificación del vehículo referido al vehículo completo.

2.38. **CardVehiclesUsed**

Información almacenada en una tarjeta de conductor o de taller relativa a los vehículos empleados por el titular de la tarjeta (anexo 1C, requisitos 270, 295, 323 y 346).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord es el índice del último registro actualizado del vehículo.

Asignación de valor: número correspondiente al numerador del registro de un vehículo. Al primer registro de la estructura se le asigna el número '0'.

cardVehicleRecords es el conjunto de registros con información sobre los vehículos utilizados.

2.39. **CardVehicleUnitRecord**

Generación 2:

Información almacenada en una tarjeta de conductor o de taller y relativa a una unidad instalada en el vehículo que ha sido utilizada (anexo 1C, requisitos 303 y 351).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                           TimeReal,
   manufacturerCode                    ManufacturerCode,
   deviceID                            INTEGER(0..255),
   vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp es el comienzo del período de uso de la unidad instalada en el vehículo (es decir, primera inserción de la tarjeta en la unidad instalada en el vehículo en el período).

manufacturerCode identifica al fabricante de la unidad instalada en el vehículo.

deviceID identifica el tipo de unidad instalada en el vehículo de un fabricante. El valor es particular del fabricante.

vuSoftwareVersion es el número de la versión de *software* que lleva instalado la unidad instalada en el vehículo.

2.40. **CardVehicleUnitsUsed**

Generación 2:

Información almacenada en una tarjeta de conductor o de taller y relativa a las unidades instaladas en el vehículo utilizadas por el titular de la tarjeta (anexo 1C, requisitos 306 y 352).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord es el índice del último registro actualizado de la unidad instalada en el vehículo.

Asignación de valor: número correspondiente al numerador del registro de una unidad instalada en el vehículo. Al primer registro de la estructura se le asigna el número '0'.

cardVehicleUnitRecords es el conjunto de registros con información sobre las unidades instaladas en el vehículo utilizadas.

2.41. **Certificate**

El certificado de una clave pública expedido por una autoridad de certificación.

Generación 1:

```
Certificate ::= OCTET STRING (SIZE(194))
```

Asignación de valor: firma digital con recuperación parcial de un CertificateContent, con arreglo al apéndice 11 «Mecanismos de seguridad comunes»: firma (128 bytes) || resto de la clave pública (58 bytes) || referencia de la autoridad de certificación (8 bytes).

Generación 2:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Asignación de valor: véase el apéndice 11.

2.42. **CertificateContent**

Generación 1:

El contenido (sin cifrar) del certificado de una clave pública, con arreglo al apéndice 11 «Mecanismos de seguridad comunes».

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier es la versión del certificado que corresponda.

Asignación de valor: '01h' para esta versión.

certificationAuthorityReference identifica a la autoridad de certificación que expide el certificado. También es una referencia a la clave pública de dicha autoridad de certificación.

certificateHolderAuthorisation identifica los derechos que asisten al titular del certificado.

certificateEndOfValidity es la fecha en que expira administrativamente el certificado.

certificateHolderReference identifica al titular del certificado. También es una referencia a su clave pública.

publicKey es la clave pública que se certifica con este certificado.

2.43. **CertificateHolderAuthorisation**

Identificación de los derechos que asisten al titular de un certificado.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Generación 1:

tachographApplicationID es el identificador de la aplicación de tacógrafo.

Asignación de valor: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Este AID es un identificador propio y no registrado de la aplicación, con arreglo a la norma ISO/CEI 7816-5.

equipmentType es la identificación del tipo de equipo al que se refiere el certificado.

Asignación de valor: de acuerdo con el tipo de datos EquipmentType. **0** si el certificado es de un Estado miembro.

Generación 2:

tachographApplicationID denota los 6 bytes más significativos del identificador de aplicación (AID) de la tarjeta de tacógrafo de generación 2. La AID de la aplicación de la tarjeta de tacógrafo se especifica en el capítulo 6.2.

Asignación de valor: 'FF 53 4D 52 44 54'.

equipmentType es la identificación del tipo de equipo según lo especificado para la generación 2 a que se refiere el certificado.

Asignación de valor: de acuerdo con el tipo de datos EquipmentType.

2.44. **CertificateRequestID**

Identificacion exclusiva de una solicitud de certificado. También puede utilizarse como identificador de la clave pública de una unidad instalada en el vehículo si en el momento de generar el certificado se desconoce el número de serie de la unidad a la que se refiere la clave.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber es un número de serie para la solicitud de certificado, exclusivo para el fabricante y para el mes a que se refiere la línea siguiente.

requestMonthYear es la identificación del mes y el año de la solicitud de certificado.

Asignación de valor: codificación BCD del mes (dos dígitos) y el año (dos últimos dígitos).

crIdentifier: es un identificador para distinguir entre una solicitud de certificado y un número de serie ampliado.

Asignación de valor: 'FFh'.

manufacturerCode: es el código numérico del fabricante que solicita el certificado.

2.45. **CertificationAuthorityKID**

Identificador de la clave pública de una autoridad de certificación (un Estado miembro o la autoridad de certificación europea).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric es el código numérico de nación de la autoridad de certificación.

nationAlpha es el código alfanumérico de nación de la autoridad de certificación.

keySerialNumber es un número de serie para distinguir las diferentes claves de la autoridad de certificación en caso de que estas se cambien.

additionalInfo es un campo de dos bytes para codificación adicional (específica de la autoridad de certificación).

caIdentifier es un identificador para distinguir entre el identificador de clave de una autoridad de certificación y otros identificadores de clave.

Asignación de valor: '01h'.

2.46. **CompanyActivityData**

Información almacenada en una tarjeta de empresa y relativa a las actividades que se realizan con la tarjeta (anexo 1C, requisitos 373 y 379).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord         INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords             SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord              SEQUENCE {
      companyActivityType                CompanyActivityType,
      companyActivityTime                TimeReal,
      cardNumberInformation              FullCardNumber,
      vehicleRegistrationInformation     VehicleRegistrationIdentification,
      downloadPeriodBegin                TimeReal,
      downloadPeriodEnd                  TimeReal
    }
}
```

companyPointerNewestRecord es el índice del último companyActivityRecord actualizado.

Asignación de valor: número correspondiente al numerador del registro de una actividad de la empresa. Al primer registro de la estructura se le asigna el número '0'.

companyActivityRecords es el conjunto de todos los registros de actividades de la empresa.

companyActivityRecord es la secuencia de información relativa a una actividad de la empresa.

companyActivityType es el tipo de actividad de la empresa.

companyActivityTime es la fecha y la hora de la actividad de la empresa.

cardNumberInformation es el número de tarjeta y el nombre del Estado miembro que ha expedido la tarjeta cuyos datos se han transferido, en tal caso.

vehicleRegistrationInformation es el VRN y el nombre del Estado miembro donde se ha matriculado el vehículo cuyos datos se han transferido o cuyo bloqueo se ha activado o desactivado.

downloadPeriodBegin y **downloadPeriodEnd** es el período transferido de la VU, en tal caso.

2.47. **CompanyActivityType**

Código que indica una actividad realizada por una empresa haciendo uso de su tarjeta de empresa.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.48. **CompanyCardApplicationIdentification**

Información almacenada en una tarjeta de empresa y relativa a la identificación de la aplicación de la tarjeta (anexo 1C, requisitos 369 y 375).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId especifica el tipo de tarjeta utilizado.

cardStructureVersion especifica la versión de la estructura que se utiliza en la tarjeta.

noOfCompanyActivityRecords es el número de registros de actividades de la empresa que puede almacenar la tarjeta.

2.49. **CompanyCardHolderIdentification**

Información almacenada en una tarjeta de empresa y relativa a la identificación del titular de dicha tarjeta (anexo 1C, requisitos 372 y 378).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName es el nombre de la empresa titular.

companyAddress es la dirección de la empresa titular.

cardHolderPreferredLanguage es el idioma preferido por el titular de la tarjeta.

2.50. **ControlCardApplicationIdentification**

Información almacenada en una tarjeta de control y relativa a la identificación de la aplicación de la tarjeta (anexo 1C, requisitos 357 y 363).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId especifica el tipo de tarjeta utilizado.

cardStructureVersion especifica la versión de la estructura que se utiliza en la tarjeta.

noOfControlActivityRecords es el número de registros de actividades de control que puede almacenar la tarjeta.

2.51. **ControlCardControlActivityData**

Información almacenada en una tarjeta de control y relativa a las actividades que se realizan con la tarjeta (anexo 1C, requisitos 361 y 367).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
     controlType                       ControlType,
     controlTime                       TimeReal,
     controlledCardNumber              FullCardNumber,
     controlledVehicleRegistration     VehicleRegistrationIdentification,
     controlDownloadPeriodBegin        TimeReal,
     controlDownloadPeriodEnd          TimeReal
    }
}
```

controlPointerNewestRecord es el índice del último registro actualizado de una actividad de control.

Asignación de valor: número correspondiente al numerador del registro de una actividad de control. Al primer registro de la estructura se le asigna el número '0'.

controlActivityRecords es el conjunto de todos los registros de actividades de control.

controlActivityRecord es la secuencia de información relativa a un control.

controlType es el tipo de control.

controlTime es la fecha y la hora del control.

controlledCardNumber es el número de tarjeta y el nombre del Estado miembro que ha expedido la tarjeta que es objeto del control.

controlledVehicleRegistration es el VRN y el nombre del Estado miembro donde se matriculó el vehículo que ha sido objeto del control.

controlDownloadPeriodBegin y **controlDownloadPeriodEnd** es el período cuyos datos se transfieren.

2.52. **ControlCardHolderIdentification**

Información almacenada en una tarjeta de control y relativa a la identificación del titular de la tarjeta (anexo 1C, requisitos 360 y 366).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                   Name,
   controlBodyAddress                Address,
   cardHolderName                    HolderName,
   cardHolderPreferredLanguage       Language
}
```

controlBodyName es el nombre del organismo de control que corresponde al titular de la tarjeta.

controlBodyAddress es la dirección del organismo de control que corresponde al titular de la tarjeta.

cardHolderName es el nombre y los apellidos del titular de la tarjeta de control.

cardHolderPreferredLanguage es el idioma preferido por el titular de la tarjeta.

2.53. **ControlType**

Código que indica las actividades realizadas durante un control. Este tipo de datos está relacionado con el anexo 1C, requisitos 126, 274, 299, 327 y 350.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Generación 1:

Asignación de valor — Alineación de octeto: 'cvpdxxxx'B (8 bits)

'c'B transferencia de los datos de la tarjeta:

'0'B: datos de la tarjeta no transferidos durante esta actividad de control,

'1'B: datos de la tarjeta transferidos durante esta actividad de control

'v'B transferencia de los datos de la VU:

'0'B: datos de la VU no transferidos durante esta actividad de control,

'1'B: datos de la VU transferidos durante esta actividad de control

'p'B impresión:

'0'B: no se imprimen datos durante esta actividad de control,

'1'B: se imprimen datos durante esta actividad de control

'd'B visualización:

'0'B: no se visualizan datos durante esta actividad de control,

'1'B: se visualizan datos durante esta actividad de control

'xxxx'B no se utiliza

Generación 2:

Asignación de valor — Alineación de octeto: 'cvpdexxx'B (8 bits)

'c'B transferencia de los datos de la tarjeta:

'0'B: datos de la tarjeta no transferidos durante esta actividad de control,

'1'B: datos de la tarjeta transferidos durante esta actividad de control

'v'B transferencia de los datos de la VU:

'0'B: datos de la VU no transferidos durante esta actividad de control,

'1'B: datos de la VU transferidos durante esta actividad de control

'p'B impresión:

'0'B: no se imprimen datos durante esta actividad de control,

'1'B: se imprimen datos durante esta actividad de control

'd'B visualización:

'0'B: no se visualizan datos durante esta actividad de control,

'1'B: se visualizan datos durante esta actividad de control

'e'B control del calibrado en carretera:

'0'B: parámetros de calibrado no controlados durante esta actividad de control,

'1'B: parámetros de calibrado controlados durante esta actividad de control,

'xxx'B RFU.

2.54. **CurrentDateTime**

La fecha y la hora actuales del aparato de control.

```
CurrentDateTime ::= TimeReal
```

Asignación de valor: no hay más especificaciones.

2.55. **CurrentDateTimeRecordArray**

Generación 2:

La fecha y la hora actuales más metadatos tal y como se utilizan en el protocolo de transferencia.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType denota el tipo de registro (CurrentDateTime). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de CurrentDateTime en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros de fecha y hora actuales.

2.56. **DailyPresenceCounter**

Contador que está almacenado en una tarjeta de conductor o de taller y que se incrementa en una unidad por cada día civil que se haya insertado la tarjeta en una VU. Este tipo de datos está relacionado con los requisitos 266, 299, 320 y 343 del anexo 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Asignación de valor: número consecutivo con un valor máximo de 9 999 y que vuelve a comenzar desde 0. La primera vez que se expide la tarjeta, el número se pone a 0.

2.57. **Datef**

Fecha expresada en un formato numérico fácil de imprimir.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Asignación de valor:

yyyy	año
mm	mes
dd	día
'00000000'H	denota explícitamente la ausencia de fecha.

2.58. **DateOfDayDownloaded**

Generación 2:

La fecha y hora de la transferencia.

```
DateOfDayDownloaded ::= TimeReal
```

Asignación de valor: no hay más especificaciones.

2.59. **DateOfDayDownloadedRecordArray**

Generación 2:

La fecha y la hora de la transferencia más metadatos tal y como se utilizan en el protocolo de transferencia.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType denota el tipo de registro (DateOfDayDownloaded). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de CurrentDateTime en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de fecha y hora de los registros de transferencia.

2.60. **Distance**

Una distancia recorrida (resultado de calcular la diferencia en kilómetros entre dos lecturas del cuentakilómetros del vehículo).

```
Distance ::= INTEGER(0..2^16-1)
```

Asignación de valor: número binario sin signo. Valor en km en el intervalo operativo de 0 a 9 999 km.

2.61. **DriverCardApplicationIdentification**

Información almacenada en una tarjeta de conductor y relativa a la identificación de la aplicación de la tarjeta (anexo 1C, requisitos 253 y 278).

Generación 1:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId especifica el tipo de tarjeta utilizado.

cardStructureVersion especifica la versión de la estructura que se utiliza en la tarjeta.

noOfEventsPerType es el número de incidentes de cada tipo que puede registrar la tarjeta.

noOfFaultsPerType es el número de fallos de cada tipo que puede registrar la tarjeta.

activityStructureLength indica el número de bytes disponibles para almacenar registros de actividad.

noOfCardVehicleRecords es el número de registros del vehículo que caben en la tarjeta.

noOfCardPlaceRecords es el número de lugares que puede registrar la tarjeta.

Generación 2:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Además de los de la generación 1, se utilizan los siguientes elementos de datos:

noOfGNSSCDRecords es el número de registros GNSS de conducción continua que puede almacenar la tarjeta.

noOfSpecificConditionRecords es el número de registros de condiciones específicas que puede almacenar la tarjeta.

2.62. DriverCardHolderIdentification

Información almacenada en una tarjeta de conductor y relativa a la identificación del titular de la tarjeta (anexo 1C, requisitos 256 y 281).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

cardHolderName es el nombre y los apellidos del titular de la tarjeta de conductor.

cardHolderBirthDate es la fecha de nacimiento del titular de la tarjeta de conductor.

cardHolderPreferredLanguage es el idioma preferido por el titular de la tarjeta.

2.63. **DSRCSecurityData**

Generación 2:

La información en texto sin formato y el MAC que deben transmitirse a través de DSRC desde el tacógrafo al interrogador remoto (RI), véanse detalles en el apéndice 11, parte B, capítulo 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength forma parte de la codificación DER-TLV y debe ponerse a '81 10' (véase el apéndice 11, parte B, capítulo 13).

currentDateTime es la fecha y la hora actuales de la unidad instalada en el vehículo.

counter enumera los mensajes RTM.

vuSerialNumber es el número de serie de la unidad instalada en el vehículo.

dSRCMKVersionNumber es el número de versión de la clave maestra DSRC de la que se derivaron las claves DSRC específicas de VU.

tagLengthMac es la etiqueta y la longitud del objeto de datos MAC como parte de la codificación DER-TLV. La etiqueta deberá ser '8E' y la longitud codificará la longitud del MAC en octetos (véase el apéndice 11, parte B, capítulo 13).

mac es el MAC calculado sobre el mensaje RTM (véase el apéndice 11, parte B, capítulo 13).

2.64. **EGFCertificate**

Generación 2:

Certificado de la clave pública del dispositivo GNSS externo para la autenticación mutua con una VU. La estructura de este certificado se especifica en el apéndice 11.

```
EGFCertificate ::= Certificate
```

2.65. **EmbedderIcAssemblerId**

Facilita información sobre el integrador del CI.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode es el código de país de dos letras del integrador del módulo conforme a la norma ISO 3166.

moduleEmbedder identifica al integrador del módulo.

manufacturerInformation para uso interno del fabricante.

2.66. **EntryTypeDailyWorkPeriod**

Código para distinguir entre el comienzo y el final cuando se introduce un período diario de trabajo, el lugar y la condición de la entrada.

Generación 1

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Asignación de valor: con arreglo a la norma ISO/CEI 8824-1.

Generación 2

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Asignación de valor: con arreglo a la norma ISO/CEI 8824-1.

2.67. **EquipmentType**

Código para distinguir diferentes tipos de equipos para la aplicación de tacógrafo.

```
EquipmentType ::= INTEGER(0..255)
```

Generación 1:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Asignación de valor: con arreglo a la norma ISO/CEI 8824-1.

El valor 0 se reserva para designar a un Estado miembro o a Europa en el campo CHA de los certificados.

Generación 2:

se utilizan los mismos valores que en la generación 1, con los siguientes añadidos:

```
--GNSS Facility                          (8),
--Remote Communication Module            (9),
--ITS interface module                   (10),
--Plaque                                 (11), -- may be used in SealRecord
--M1/N1 Adapter                          (12), -- may be used in SealRecord
--European Root CA (ERCA)                (13),
--Member State CA (MSCA)                 (14),
--External GNSS connection               (15), -- may be used in SealRecord
--Unused                                 (16), -- used in SealDataVu
--RFU                                    (17..255)
```

Nota: Pueden utilizarse en SealRecord, si procede, los valores de generación 2 de la placa, el adaptador y la conexión del GNSS externo, así como los valores de generación 1 de la unidad instalada en el vehículo y el sensor de movimiento.

2.68. **EuropeanPublicKey**

Generación 1:

La clave pública europea.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Código que explica por qué se ha registrado un incidente o fallo.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Asignación de valor:

'00'H	uno de los diez incidentes o fallos más recientes (o de los diez últimos)
'01'H	el incidente de más duración ocurrido en uno de los diez últimos días en que se hayan producido incidentes de este tipo
'02'H	uno de los cinco incidentes de más duración ocurridos en los últimos 365 días
'03'H	el último incidente ocurrido en uno de los diez últimos días en que se hayan producido incidentes de este tipo
'04'H	el incidente más grave en uno de los diez últimos días en que se hayan producido incidentes de este tipo
'05'H	uno de los cinco incidentes más graves ocurridos en los últimos 365 días
'06'H	el primer incidente o fallo ocurrido tras el último calibrado
'07'H	un incidente o fallo activo/en curso
'08'H to '7F'H	RFU
'80'H to 'FF'H	específica del fabricante

2.70. **EventFaultType**

Código que califica un incidente o un fallo.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Asignación de valor:

Generación 1:

'0x'H	Incidentes de carácter general,
'00'H	No hay más información,
'01'H	Inserción de una tarjeta no válida,
'02'H	Conflicto de tarjetas,
'03'H	Solapamiento temporal,
'04'H	Conducción sin tarjeta adecuada,
'05'H	Inserción de tarjeta durante la conducción,
'06'H	Error al cerrar la última sesión de la tarjeta,
'07'H	Exceso de velocidad,
'08'H	Interrupción del suministro eléctrico,
'09'H	Error en datos de movimiento,
'0A'H	Conflicto de movimiento del vehículo,
'0B' to '0F'H	RFU,

	Intentos de violación de la seguridad relacionados con la VU,
‘1x’H	No hay más información,
‘10’H	Fallo de autenticación del sensor de movimiento,
‘11’H	Fallo de autenticación de la tarjeta de tacógrafo,
‘12’H	Cambio no autorizado del sensor de movimiento,
‘13’H	Error de integridad en la entrada de los datos de la tarjeta,
‘14’H	Error de integridad en los datos de usuario almacenados,
‘15’H	Error en una transferencia interna de datos,
‘16’H	Apertura no autorizada de la carcasa,
‘17’H	Sabotaje del hardware,
‘18’H	RFU,
‘19’H to ‘1F’H	
‘2x’H	Intentos de violación de la seguridad relacionados con el sensor,
‘20’H	No hay más información,
‘21’H	Fallo de autenticación,
‘22’H	Error de integridad en los datos almacenados,
‘23’H	Error en una transferencia interna de datos,
‘24’H	Apertura no autorizada de la carcasa,
‘25’H	Sabotaje del hardware,
‘26’H to ‘2F’H	RFU,
‘3x’H	Fallos del aparato de control,
‘30’H	No hay más información,
‘31’H	Fallo interno de la VU,
‘32’H	Fallo de la impresora,
‘33’H	Fallo de la pantalla,
‘34’H	Fallo de transferencia,
‘35’H	Fallo del sensor,
‘36’H to ‘3F’H	RFU,
‘4x’H	Fallos de las tarjetas,
‘40’H	No hay más información,
‘41’H to ‘4F’H	RFU,
‘50’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	específicos del fabricante.

Generación 2:

se utilizan los mismos valores que en la generación 1, con los siguientes añadidos:

‘0B’H	Conflicto temporal (entre el GNSS y el reloj interno de la VU),
‘0C’ to ‘0F’H	RFU,
‘5x’H	Fallos relacionados con el GNSS,
‘50’H	No hay más información,
‘51’H	Fallo del receptor GNSS interno,
‘52’H	Fallo del receptor GNSS externo,
‘53’H	Fallo del dispositivo de comunicación GNSS externo,
‘54’H	Ausencia de datos de posición GNSS,
‘55’H	Detección de manipulación de GNSS,
‘56’H	Certificado del dispositivo GNSS externo expirado,
‘57’H to ‘5F’H	RFU,
‘6x’H	Fallos relacionados con el módulo de comunicación a distancia,
‘60’H	No hay más información,
‘61’H	Fallo del módulo de comunicación a distancia,
‘62’H	Fallo de comunicación del módulo de comunicación a distancia,
‘63’H to ‘6F’H	RFU,
‘7x’H	Fallos de la interfaz ITS,
‘70’H	No hay más información,
‘71’H to ‘7F’H	RFU.

2.71. **ExtendedSealIdentifier**

Generación 2:

El identificador de precinto ampliado identifica de manera única un precinto (anexo 1C, requisito 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode es un código del fabricante del precinto.

sealIdentifier es un identificador del precinto que es exclusivo para el fabricante.

2.72. **ExtendedSerialNumber**

Identificación exclusiva de un equipo. También puede utilizarse como el identificador de clave pública de un equipo.

Generación 1:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber es el número de serie de un equipo; exclusivo para el fabricante, para el tipo de equipo y para el mes y año a que se refiere la línea siguiente.

monthYear es la identificación del mes y el año de fabricación (o de la asignación del número de serie).

Asignación de valor: codificación BCD del mes (dos dígitos) y el año (dos últimos dígitos).

type es un identificador del tipo de equipo.

Asignación de valor: específica del fabricante, con 'FFh' valor reservado.

manufacturerCode: es el código numérico que identifica al fabricante de un equipo homologado.

Generación 2:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                EquipmentType,
   manufacturerCode                    ManufacturerCode
}
```

serialNumber véase generación 1

monthYear véase generación 1

type indica el tipo de equipo

manufacturerCode: véase generación 1.

2.73. **FullCardNumber**

Código que identifica por completo a una tarjeta de tacógrafo.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType es el tipo de tarjeta de tacógrafo.

cardIssuingMemberState es el código del Estado miembro que ha expedido la tarjeta.

cardNumber es el número de la tarjeta.

2.74. **FullCardNumberAndGeneration**

Generación 2:

Código que identifica por completo a una tarjeta de tacógrafo y su generación.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identifica la tarjeta de tacógrafo.

generation indica la generación de la tarjeta de tacógrafo utilizada.

2.75. **Generation**

Generación 2:

Indica la generación del tacógrafo utilizado.

```
Generation ::= INTEGER(0..255)
```

Asignación de valor:

'00'H	RFU
'01'H	Generación 1
'02'H	Generación 2
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

Generación 2:

Las coordenadas geográficas se codifican con números enteros. Estos enteros son múltiplos de la codificación ± GGMM.M para la latitud y ± GGGMM.M para la longitud, donde ± GG y ± GGG denotan los grados y MM.M los minutos.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude se codifica como un múltiplo (factor 10) de la representación ± GGMM.M.

longitude se codifica como un múltiplo (factor 10) de la representación ± GGGMM.M.

2.77. **GNSSAccuracy**

Generación 2:

La exactitud de los datos de posición del GNSS (definición eee)). Esta exactitud se codifica con un número entero y es un múltiplo (factor 10) del valor X.Y facilitado por la sentencia GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Generación 2:

Información almacenada en una tarjeta de conductor o de taller y relativa a la posición GNSS del vehículo si el tiempo de conducción continua del conductor alcanza un múltiplo de tres horas (anexo 1C, requisitos 306 y 354).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord es el índice del último registro actualizado de conducción continua del GNSS.

Asignación de valor: número correspondiente al numerador del registro de conducción continua del GNSS. Al primer registro de la estructura se le asigna el número '0'.

gnssContinuousDrivingRecords es el conjunto de registros que contienen la fecha y hora en que la conducción continua alcanza un múltiplo de tres horas e información sobre la posición del vehículo.

2.79. **GNSSContinuousDrivingRecord**

Generación 2:

Información almacenada en una tarjeta de conductor o de taller y relativa a la posición GNSS del vehículo si el tiempo de conducción continua del conductor alcanza un múltiplo de tres horas (anexo 1C, requisitos 305 y 353).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssPlaceRecord                      GNSSPlaceRecord
}
```

timeStamp es la fecha y hora en las que el tiempo de conducción continua del titular de la tarjeta llega a un múltiplo de tres horas.

gnssPlaceRecord contiene información relacionada con la posición del vehículo.

2.80. **GNSSPlaceRecord**

Generación 2:

Información relacionada con la posición GNSS del vehículo (anexo 1C, requisitos 108, 109, 110, 296, 305, 347 y 353).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                            TimeReal,
   gnssAccuracy                         GNSSAccuracy,
   geoCoordinates                       GeoCoordinates
}
```

timeStamp es la fecha y la hora en que se determinó la posición GNSS del vehículo.

gnssAccuracy es la exactitud de los datos de posición GNSS.

geoCoordinates es la localización registrada utilizando el GNSS.

2.81. **HighResOdometer**

Lectura del cuentakilómetros del vehículo: distancia acumulada que ha recorrido el vehículo durante su funcionamiento.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Asignación de valor: número binario sin signo. Valor en 1/200 km en el intervalo operativo de 0 a 21 055 406 km.

2.82. **HighResTripDistance**

La distancia recorrida durante todo o parte de un viaje.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Asignación de valor: número binario sin signo. Valor en 1/200 km en el intervalo operativo de 0 a 21 055 406 km.

2.83. **HolderName**

El nombre y apellidos del titular de una tarjeta.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname son los apellidos del titular. No incluye el tratamiento.

Asignación de valor: cuando una tarjeta no es personal, holderSurname contiene la misma información que companyName o workshopName o controlBodyName.

holderFirstNames es el nombre y las iniciales del titular.

2.84. **InternalGNSSReceiver**

Generación 2:

Información sobre si el receptor GNSS es interno o externo a la unidad instalada en el vehículo. True significa que el receptor GNSS es interno a la VU. False significa que el receptor GNSS es externo.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Constante del aparato de control [definición m)].

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Asignación de valor: impulsos por kilómetro en el intervalo operativo de 0 a 64 255 impulsos/km.

2.86. **KeyIdentifier**

Un identificador exclusivo de una clave pública, empleado para hacer referencia a dicha clave y seleccionarla. También identifica al titular de la clave.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber                ExtendedSerialNumber,
   certificateRequestID                CertificateRequestID,
   certificationAuthorityKID           CertificationAuthorityKID
}
```

La primera opción sirve para hacer referencia a la clave pública de una unidad instalada en el vehículo o de una tarjeta de tacógrafo.

La segunda opción sirve para hacer referencia a la clave pública de una VU (en caso de que el número de serie de dicha VU no pueda conocerse en el momento de generarse el certificado).

La tercera opción sirve para hacer referencia a la clave pública de un Estado miembro.

2.87. **KMWCKey**

Generación 2:

Clave AES y su versión de clave asociada utilizada en el emparejamiento VU — sensor de movimiento. Para más detalles véase el apéndice 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey es la longitud de la clave AES concatenada con la clave que se utiliza para el emparejamiento VU — sensor de movimiento.

keyVersion denota la versión de la clave AES.

2.88. **Language**

Código que identifica un idioma.

```
Language ::= IA5String(SIZE(2))
```

Asignación de valor: codificación mediante dos letras en minúsculas con arreglo a la norma ISO 639.

2.89. **LastCardDownload**

Fecha y hora, almacenadas en una tarjeta de conductor, de la última transferencia de los datos de la tarjeta (para fines distintos de los de control), anexo 1C, requisitos 257 y 282. Esta fecha puede ser actualizada por una VU o por cualquier lector de tarjetas.

```
LastCardDownload ::= TimeReal
```

Asignación de valor: no hay más especificaciones.

2.90. **LinkCertificate**

Generación 2:

Certificado de enlace entre pares de claves de la European Root CA.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Circunferencia efectiva de los neumáticos de las ruedas [definición u)].

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

Asignación de valor: número binario sin signo, valor en 1/8 mm en el intervalo operativo de 0 a 8 031 mm.

2.92. **MAC**

Generación 2:

Una suma de control criptográfica de 8, 12 o 16 bytes de longitud correspondiente a los conjuntos de cifrado que se especifican en el apéndice 11.

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Código que indica si el titular de una tarjeta, en el momento de insertar dicha tarjeta, ha introducido o no manualmente alguna actividad del conductor (anexo 1B, requisito 081, y anexo 1C, requisito 102).

```
ManualInputFlag ::= INTEGER {
   noEntry                              (0)
   manualEntries                        (1)
}
```

Asignación de valor: no hay más especificaciones.

2.94. **ManufacturerCode**

Código que identifica al fabricante de un aparato homologado.

```
ManufacturerCode ::= INTEGER(0..255)
```

El laboratorio encargado de los ensayos de interoperabilidad conservará y publicará en su sitio web la lista de códigos de fabricantes (anexo 1C, requisito 454).

Los códigos de fabricante se asignarán provisionalmente a los desarrolladores de tacógrafos al presentar una solicitud al laboratorio competente para realizar los ensayos de interoperabilidad.

2.95. **ManufacturerSpecificEventFaultData**

Generación 2:

Los códigos de error específicos del fabricante simplifican el análisis de errores y el mantenimiento de las VU.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode identifica al fabricante de la unidad instalada en el vehículo.

manufacturerSpecificErrorCode es un código de error específico del fabricante.

2.96. **MemberStateCertificate**

El certificado de la clave pública de un Estado miembro, expedido por la autoridad de certificación europea.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Generación 2:

El certificado del Estado miembro más metadatos tal y como se utilizan en el protocolo de transferencia.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType denota el tipo de registro (MemberStateCertificate). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de MemberStateCertificate en bytes.

noOfRecords es el número de registros que hay en el conjunto. El valor se pondrá a 1, ya que los certificados pueden tener diferentes longitudes.

records es el conjunto de certificados de Estado miembro.

2.98. **MemberStatePublicKey**

Generación 1:

La clave pública de un Estado miembro.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Un nombre.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage especifica un conjunto de caracteres definidos en el capítulo 4,

name representa un nombre codificado utilizando el conjunto de caracteres especificado.

2.100. **NationAlpha**

Toda referencia alfabética a un país se realizará con arreglo a los distintivos utilizados en los vehículos en el tráfico internacional (Convención de Viena sobre la circulación vial de las Naciones Unidas, 1968).

```
NationAlpha ::= IA5String(SIZE(3))
```

Los códigos alfanuméricos que identifican a los distintos países figurarán en una lista mantenida en el sitio web del laboratorio designado para realizar los ensayos de interoperabilidad, tal y como establece en el anexo 1C, requisito 440.

2.101. **NationNumeric**

Referencia numérica a un país.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Asignación de valor: véase tipo de datos 2.100 (NationAlpha).

Toda modificación o actualización de la especificación alfanumérica relativa a los distintos países descrita en el párrafo anterior tendrá lugar, únicamente, después de que el laboratorio designado haya obtenido las observaciones de los fabricantes de unidades instaladas en el vehículo de tacógrafos digitales e inteligentes homologados.

2.102. **NoOfCalibrationRecords**

Número de registros de calibrado que puede almacenar una tarjeta de taller.

Generación 1:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Asignación de valor: véase el apéndice 2.

Generación 2:

$$\texttt{NoOfCalibrationRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Asignación de valor: véase el apéndice 2.

2.103. **NoOfCalibrationsSinceDownload**

Contador que indica el número de calibrados realizados con una tarjeta de taller desde que se transfirieran por última vez sus datos (anexo 1C, requisitos 317 y 340).

$$\texttt{NoOfCalibrationsSinceDownload ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Asignación de valor: no hay más especificaciones.

2.104. **NoOfCardPlaceRecords**

Número de registros de lugares que puede almacenar una tarjeta de conductor o de taller.

Generación 1:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Asignación de valor: véase el apéndice 2.

Generación 2:

$$\texttt{NoOfCardPlaceRecords ::= INTEGER(0..}2^{16}\texttt{-1)}$$

Asignación de valor: véase el apéndice 2.

2.105. **NoOfCardVehicleRecords**

Número de registros sobre vehículos usados que puede almacenar una tarjeta de conductor o de taller.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Asignación de valor: véase el apéndice 2.

2.106. **NoOfCardVehicleUnitRecords**

Generación 2:

Número de registros sobre unidades instalas en vehículos usados que puede almacenar una tarjeta de conductor o de taller.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Asignación de valor: véase el apéndice 2.

2.107. **NoOfCompanyActivityRecords**

Número de registros sobre actividades de empresa que puede almacenar una tarjeta de empresa.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Asignación de valor: véase el apéndice 2.

2.108. **NoOfControlActivityRecords**

Número de registros sobre actividades de control que puede almacenar una tarjeta de control.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Asignación de valor: véase el apéndice 2.

2.109. **NoOfEventsPerType**

Número de incidentes de cada tipo que puede almacenar una tarjeta.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Asignación de valor: véase el apéndice 2.

2.110. **NoOfFaultsPerType**

Número de fallos de cada tipo que puede almacenar una tarjeta.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Asignación de valor: véase el apéndice 2.

2.111. **NoOfGNSSCDRecords**

Generación 2:

Número de registros GNSS de conducción continua que puede almacenar una tarjeta.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Asignación de valor: véase el apéndice 2.

2.112. **NoOfSpecificConditionRecords**

Generación 2:

Número de registros de condición específica que puede almacenar una tarjeta.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Asignación de valor: véase el apéndice 2.

2.113. **OdometerShort**

Lectura del cuentakilómetros del vehículo en forma abreviada.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Asignación de valor: número binario sin signo. Valor en km en el intervalo operativo de 0 a 9 999 999 km.

2.114. **OdometerValueMidnight**

La lectura del cuentakilómetros del vehículo a medianoche de un día determinado (anexo 1B, requisito 090, y anexo 1C, requisito 113).

```
OdometerValueMidnight ::= OdometerShort
```

Asignación de valor: no hay más especificaciones.

2.115. **OdometerValueMidnightRecordArray**

Generación 2:

El OdometerValueMidnight más metadatos tal como se utilizan en el protocolo de transferencia.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType denota el tipo de registro (OdometerValueMidnight). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de OdometerValueMidnight en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros de OdometerValueMidnight.

2.116. **OverspeedNumber**

Número de incidentes de exceso de velocidad ocurridos desde el último control del exceso de velocidad.

```
OverspeedNumber ::= INTEGER(0..255)
```

Asignación de valor: 0 significa que no se ha producido ningún incidente de exceso de velocidad desde el último control, 1 significa que se ha producido un incidente de exceso de velocidad desde el último control … 255 significa que se han producido 255 o más incidentes de exceso de velocidad desde el último control.

2.117. **PlaceRecord**

Información relativa al lugar donde comienza o termina un período de trabajo diario (anexo 1C, requisitos 108, 271, 296, 324 y 347).

Generación 1:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime es una fecha y una hora relacionadas con la entrada.

entryTypeDailyWorkPeriod es el tipo de entrada.

dailyWorkPeriodCountry es el país introducido.

dailyWorkPeriodRegion es la región introducida.

vehicleOdometerValue es la lectura del cuentakilómetros en el momento de introducir el lugar.

Generación 2:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort,
   entryGNSSPlaceRecord               GNSSPlaceRecord
}
```

Además de los de la generación 1, se utiliza el siguiente componente:

entryGNSSPlaceRecord es la localización y la hora registrada.

2.118. **PreviousVehicleInfo**

Información relativa al vehículo que utilizara previamente un conductor al insertar su tarjeta en una unidad instalada en el vehículo (anexo 1B, requisito 081, y anexo 1C, requisito 102).

Generación 1:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification es el VRN y el nombre del Estado miembro donde se matriculara el vehículo.

cardWithdrawalTime es la fecha y la hora de extracción de la tarjeta.

Generación 2:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Además de los de la generación 1, se utiliza el siguiente elemento de datos:

vuGeneration indica la generación de la unidad instalada en el vehículo.

2.119. **PublicKey**

Generación 1:

Una clave RSA pública.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus es el módulo del par de claves.

rsaKeyPublicExponent es el exponente público del par de claves.

2.120. **RecordType**

Generación 2:

Referencia a un tipo de registro. Este tipo de datos se utiliza en RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Asignación de valor:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	RFU,
'80'H to 'FF'H	específicos del fabricante.

2.121. **RegionAlpha**

Referencia alfabética a una región perteneciente a un país especificado.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Generación 1:

Asignación de valor:

```
'   '        No information available,
Spain:
'AN '        Andalucía,
'AR '        Aragón,
'AST'        Asturias,
'C  '        Cantabria,
'CAT'        Cataluña,
'CL '        Castilla-León,
'CM '        Castilla-La-Mancha,
'CV'         Valencia,
'EXT'        Extremadura,
'G  '        Galicia,
'IB '        Baleares,
'IC '        Canarias,
'LR '        La Rioja,
'M  '        Madrid,
'MU '        Murcia,
'NA '        Navarra,
'PV '        País Vasco
```

Generación 2:

Los códigos alfabéticos que identifican a las distintas regiones figurarán en una lista mantenida en el sitio web del laboratorio designado para realizar los ensayos de interoperabilidad.

2.122. **RegionNumeric**

Referencia numérica a una región perteneciente a un país especificado.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Generación 1:

Asignación de valor:

```
'00'H        No information available,
Spain:
'01'H        Andalucía,
'02'H        Aragón,
'03'H        Asturias,
'04'H        Cantabria,
'05'H        Cataluña,
'06'H        Castilla-León,
'07'H        Castilla-La-Mancha,
'08'H        Valencia,
'09'H        Extremadura,
'0A'H        Galicia,
'0B'H        Baleares,
'0C'H        Canarias,
'0D'H        La Rioja,
'0E'H        Madrid,
'0F'H        Murcia,
'10'H        Navarra,
'11'H        País Vasco
```

Generación 2:

Los códigos numéricos que identifican a las distintas regiones figurarán en una lista mantenida en el sitio web del laboratorio designado para realizar los ensayos de interoperabilidad.

2.123. **RemoteCommunicationModuleSerialNumber**

Generación 2:

número de serie del módulo de comunicación a distancia,

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Generación 1:

El módulo de un par de claves RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Asignación de valor: no especificado.

2.125. **RSAKeyPrivateExponent**

Generación 1:

El exponente privado de un par de claves RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Asignación de valor: no especificado.

2.126. **RSAKeyPublicExponent**

Generación 1:

El exponente público de un par de claves RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Asignación de valor: no especificado.

2.127. **RtmData**

Generación 2:

Para la definición de este tipo de datos, véase el apéndice 14.

2.128. **SealDataCard**

Generación 2:

Este tipo de datos almacena información sobre los precintos colocados en los distintos componentes de un vehículo y se destina al almacenamiento en una tarjeta. Este tipo de datos está relacionado con el anexo 1C, requisito 337.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                        INTEGER(1..5),
   sealRecords                            SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords es el número de registros que hay en sealRecords.

sealRecords es un conjunto de registros sobre precintos.

2.129. **SealDataVu**

Generación 2:

Este tipo de datos almacena información sobre los precintos colocados en los distintos componentes de un vehículo y se destina al almacenamiento en una unidad instalada en el vehículo.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                            SealRecord
}
```

sealRecords es un conjunto de registros sobre precintos. Si hay menos de cinco precintos, el valor de EquipmentType en todos los sealRecords no utilizados se pondrá a 16, es decir, sin utilizar.

2.130. **SealRecord**

Generación 2:

Este tipo de datos almacena información sobre un precinto colocado en un componente. Este tipo de datos está relacionado con el anexo 1C, requisito 337.

```
SealRecord ::= SEQUENCE {
   equipmentType                          EquipmentType,
   extendedSealIdentifier                 ExtendedSealIdentifier
}
```

equipmentType identifica el tipo de aparato en que se coloca el precinto.

extendedSealIdentifier es el identificador del precinto colocado en el aparato.

2.131. **SensorApprovalNumber**

Número de homologación del sensor.

Generación 1:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Asignación de valor: no especificado.

Generación 2:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Asignación de valor:

El número de homologación deberá constar según haya sido publicado en el correspondiente sitio web de la Comisión Europea, es decir, por ejemplo, incluyendo guiones si los lleva. El número de homologación deberá estar alineado a la izquierda.

2.132. **SensorExternalGNSSApprovalNumber**

Generación 2:

número de homologación del dispositivo GNSS externo.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Asignación de valor:

El número de homologación deberá constar según haya sido publicado en el correspondiente sitio web de la Comisión Europea, es decir, por ejemplo, incluyendo guiones si los lleva. El número de homologación deberá estar alineado a la izquierda.

2.133. **SensorExternalGNSSCoupledRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a la identificación del sensor de movimiento acoplado a dicha unidad (anexo 1C, requisito 100).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber es el número de serie del dispositivo GNSS externo que está acoplado a la VU.

sensorApprovalNumber es el número de homologación de este dispositivo GNSS externo.

sensorCouplingDate es la fecha de acoplamiento del dispositivo GNSS externo con la VU.

2.134. **SensorExternalGNSSIdentification**

Generación 2:

Información relativa a la identificación del dispositivo GNSS externo (anexo 1C, requisito 98).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber es el número de serie ampliado del dispositivo GNSS externo.

sensorApprovalNumber es el número de homologación del dispositivo GNSS externo.

sensorSCIdentifier es el identificador del componente de seguridad del dispositivo GNSS externo.

sensorOSIdentifier es el identificador del sistema operativo del dispositivo GNSS externo.

2.135. **SensorExternalGNSSInstallation**

Generación 2:

Información almacenada en un dispositivo GNSS externo y relativa a la instalación del sensor GNSS externo (anexo 1C, requisito 123).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst es la fecha del primer acoplamiento del dispositivo GNSS externo con una VU.

firstVuApprovalNumber es el número de homologación de la primera VU acoplada con el dispositivo GNSS externo.

firstVuSerialNumber es el número de serie de la primera VU acoplada con el dispositivo GNSS externo.

sensorCouplingDateCurrent es la fecha del acoplamiento actual del dispositivo GNSS externo con una VU.

currentVuApprovalNumber es el número de homologación de la VU actualmente acoplada con el dispositivo GNSS externo.

currentVUSerialNumber es el número de serie de la VU actualmente acoplada con el dispositivo GNSS externo.

2.136. **SensorExternalGNSSOSIdentifier**

Generación 2:

Identificador del sistema operativo del dispositivo GNSS externo.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Asignación de valor: específica del fabricante.

2.137. **SensorExternalGNSSSCIdentifier**

Generación 2:

Este tipo se utiliza, por ejemplo, para identificar el módulo criptográfico del dispositivo GNSS externo.

Identificador del componente de seguridad del dispositivo GNSS externo.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Asignación de valor: específica del fabricante del componente.

2.138. **SensorGNSSCouplingDate**

Generación 2:

Fecha de un acoplamiento entre el dispositivo GNSS externo y una unidad instala en el vehículo.

```
SensorGNSSCouplingDate ::= TimeReal
```

Asignación de valor: No especificado.

2.139. **SensorGNSSSerialNumber**

Generación 2:

Este tipo se utiliza para almacenar el número de serie del receptor GNSS tanto cuando esté dentro de la VU como cuando esté fuera de la VU.

Número de serie del receptor GNSS.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Información almacenada en un sensor de movimiento y relativa a la identificación de dicho sensor (anexo 1B, requisito 077 y anexo 1C, requisito 95).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorSCIdentifier                  SensorSCIdentifier,
   sensorOSIdentifier                  SensorOSIdentifier
}
```

sensorSerialNumber es el número de serie ampliado del sensor de movimiento (incluye el número de pieza y el código del fabricante).

sensorApprovalNumber es el número de homologación del sensor de movimiento.

sensorSCIdentifier es el identificador del componente de seguridad del sensor de movimiento.

sensorOSIdentifier es el identificador del sistema operativo del sensor de movimiento.

2.141. **SensorInstallation**

Información almacenada en un sensor de movimiento y relativa a la instalación de dicho sensor (anexo 1B, requisito 099 y anexo 1C, requisito 122).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst              SensorPairingDate,
   firstVuApprovalNumber               VuApprovalNumber,
   firstVuSerialNumber                 VuSerialNumber,
   sensorPairingDateCurrent            SensorPairingDate,
   currentVuApprovalNumber             VuApprovalNumber,
   currentVUSerialNumber               VuSerialNumber
}
```

sensorPairingDateFirst es la fecha del primer emparejamiento del sensor de movimiento con una VU.

firstVuApprovalNumber es el número de homologación de la primera VU emparejada con el sensor de movimiento.

firstVuSerialNumber es el número de serie de la primera VU emparejada con el sensor de movimiento.

sensorPairingDateCurrent es la fecha del emparejamiento actual entre el sensor de movimiento y la VU.

currentVuApprovalNumber es el número de homologación de la VU que está emparejada actualmente con el sensor de movimiento.

currentVUSerialNumber es el número de serie de la VU que está emparejada actualmente con el sensor de movimiento.

2.142. **SensorInstallationSecData**

Información almacenada en una tarjeta de taller y relativa a los datos de seguridad necesarios para emparejar sensores de movimiento y unidades instaladas en vehículos (anexo 1C, requisitos 308 y 331).

Generación 1:

```
SensorInstallationSecData ::= TdesSessionKey
```

Asignación de valor: con arreglo a la norma ISO 16844-3.

Generación 2:

Tal como se describe en el apéndice 11, una tarjeta de taller deberá almacenar hasta tres claves de emparejamiento del sensor de movimiento con la VU. Estas claves tienen diferentes versiones de clave.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Identificador del sistema operativo del sensor de movimiento.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Asignación de valor: específica del fabricante.

2.144. **SensorPaired**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a la identificación del sensor de movimiento emparejado con dicha unidad (anexo 1B, requisito 079).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDateFirst                SensorPairingDate
}
```

sensorSerialNumber es el número de serie del sensor de movimiento que está emparejado actualmente con la VU.

sensorApprovalNumber es el número de homologación del sensor de movimiento que está emparejado actualmente con la VU.

sensorPairingDateFirst es la fecha en que el sensor de movimiento emparejado actualmente a la VU se emparejó por primera vez con la VU.

2.145. **SensorPairedRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a la identificación de un sensor de movimiento emparejado con dicha unidad (anexo 1C, requisito 97).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber es el número de serie de un sensor de movimiento emparejado con la VU.

sensorApprovalNumber es el número de homologación de este sensor de movimiento.

sensorPairingDate es la fecha del emparejamiento de este sensor de movimiento con la VU.

2.146. **SensorPairingDate**

Fecha de un emparejamiento del sensor de movimiento con una VU.

```
SensorPairingDate ::= TimeReal
```

Asignación de valor: no especificado.

2.147. **SensorSCIdentifier**

Identificador del componente de seguridad del sensor de movimiento.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Asignación de valor: específica del fabricante del componente.

2.148. **SensorSerialNumber**

Número de serie del sensor de movimiento.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Una firma digital.

Generación 1:

```
Signature ::= OCTET STRING (SIZE(128))
```

Asignación de valor: con arreglo a lo dispuesto en el apéndice 11 (Mecanismos de seguridad comunes).

Generación 2:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Asignación de valor: con arreglo a lo dispuesto en el apéndice 11 (Mecanismos de seguridad comunes).

2.150. **SignatureRecordArray**

Generación 2:

Conjunto de firmas más metadatos tal como se utilizan en el protocolo de transferencia.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType denota el tipo de registro (Signature). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de Signature en bytes.

noOfRecords es el número de registros que hay en el conjunto. El valor se pondrá a 1, ya que las firmas pueden tener diferentes longitudes.

records es el conjunto de firmas.

2.151. **SimilarEventsNumber**

El número de incidentes similares de un día determinado (anexo 1B, requisito 094, y anexo 1C, requisito 117).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Asignación de valor: el 0 no se utiliza, el 1 significa que ese día solo ha ocurrido y se ha almacenado un incidente de ese tipo, el 2 significa que ese día han ocurrido 2 incidentes de ese tipo (y solo se ha almacenado uno), … 255 significa que ese día han ocurrido 255 o más incidentes de ese tipo.

2.152. **SpecificConditionRecord**

Información almacenada en una tarjeta de conductor o de taller o en una unidad instalada en el vehículo y relativa a una condición específica (anexo 1C, requisitos 130, 276, 301, 328 y 355).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   specificConditionType               SpecificConditionType
}
```

entryTime es la fecha y la hora de la entrada.

specificConditionType es el código que identifica la condición específica.

2.153. **SpecificConditions**

Información almacenada en una tarjeta de conductor o de taller o en una unidad instalada en el vehículo y relativa a una condición específica (anexo 1C, requisitos 131, 277, 302, 329 y 356).

Generación 2:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

controlPointerNewestRecord es el índice del último registro actualizado de una condición específica.

Asignación de valor: número correspondiente al numerador del registro de condición específica. Al primer registro de la estructura se le asigna el número '0'.

specificConditionRecords es el conjunto de registros con información sobre las condiciones específicas utilizadas.

2.154. **SpecificConditionType**

Código que identifica una condición específica (anexo 1B, requisitos 050b, 105a, 212a y 230a y anexo 1C, requisito 62).

```
SpecificConditionType ::= INTEGER(0..255)
```

Generación 1:

Asignación de valor:

'00'H	RFU
'01'H	Fuera de ámbito — Comienzo
'02'H	Fuera de ámbito — Final
'03'H	Trayecto en transbordador/tren
'04'H .. 'FF'H	RFU

Generación 2:

Asignación de valor:

'00'H	RFU
'01'H	Fuera de ámbito — Comienzo
'02'H	Fuera de ámbito — Final
'03'H	Trayecto en transbordador/tren — Comienzo
'04'H	Trayecto en transbordador/tren — Final
'05'H .. 'FF'H	RFU

2.155. **Speed**

Velocidad del vehículo (km/h).

```
Speed ::= INTEGER(0..255)
```

Asignación de valor: kilómetros por hora en el intervalo operativo de 0 a 220 km/h.

2.156. **SpeedAuthorised**

Velocidad máxima autorizada para el vehículo [definición hh)].

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Velocidad media en un lapso de tiempo previamente definido (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Velocidad máxima medida en un lapso de tiempo previamente definido.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Generación 2:

Para la definición de este tipo de datos, véase el apéndice 14.

2.160. **TachographPayloadEncrypted**

Generación 2:

Carga útil del tacógrafo cifrado DER-TLV, es decir, los datos enviados cifrados en el mensaje RTM. Para el cifrado, véase el apéndice 11, parte B, capítulo 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag forma parte de la codificación DER-TLV y debe ponerse a '87' (véase el apéndice 11, parte B, capítulo 13).

length es parte de la codificación DER-TLV y codificará la longitud del siguiente paddingContentIndicatorByte y el encryptedData.

paddingContentIndicatorByte deberá ser '00'.

encryptedData es la tachographPayload cifrada, según lo especificado en el apéndice 11, parte B, capítulo 13. La longitud de estos datos en octetos siempre deberá ser múltiplo de 16.

2.161. **TDesSessionKey**

Generación 1:

Una clave de sesión triple DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Asignación de valor: no hay más especificaciones.

2.162. **TimeReal**

Código para un campo combinado de fecha y hora, donde ambos parámetros se expresan como los segundos transcurridos desde las 00h00m00s del 1 de enero de 1970, tiempo medio de Greenwich.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Asignación de valor — Alineación de octeto: número de segundos transcurridos a partir de la medianoche del día 1 de enero de 1970, tiempo medio de Greenwich.

La fecha/hora máxima posible es en el año 2106.

2.163. **TyreSize**

Designación de las dimensiones de los neumáticos.

```
TyreSize ::= IA5String(SIZE(15))
```

Asignación de valor: de conformidad con la Directiva 92/23/CEE de 31 de marzo de 1992 (DO L 129 de 14.5.1992, p. 95).

2.164. **VehicleIdentificationNumber**

Número de identificación del vehículo (VIN) referido al vehículo completo, generalmente el número de serie del chasis o el número de bastidor.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Asignación de valor: tal y como se define en la norma ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Generación 2:

El VehicleIdentificationNumber más metadatos tal como se utilizan en el protocolo de transferencia.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType denota el tipo de registro (VehicleIdentificationNumber). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VehicleIdentificationNumber en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de números de identificación de vehículos.

2.166. **VehicleRegistrationIdentification**

Identificación de un vehículo, exclusiva para Europa (VRN y Estado miembro).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation es la nación donde se matriculó el vehículo.

vehicleRegistrationNumber es el número de matrícula del vehículo (VRN).

2.167. **VehicleRegistrationNumber**

Número de matrícula del vehículo (VRN). El número de matrícula lo asigna la autoridad de matriculación de vehículos.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   vehicleRegNumber                    OCTET STRING (SIZE(13))
}
```

codePage especifica un conjunto de caracteres definidos en el capítulo 4,

vehicleRegNumber representa un VRN codificado utilizando el conjunto de caracteres especificado.

Asignación de valor: específica para cada país.

2.168. **VehicleRegistrationNumberRecordArray**

Generación 2:

El VehicleRegistrationNumber más metadatos tal como se utilizan en el protocolo de transferencia.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleRegistrationNumber
}
```

recordType denota el tipo de registro (VehicleRegistrationNumber). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VehicleRegistrationNumber en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de números de matrícula de vehículos.

2.169. **VuAbility**

Generación 2:

Información almacenada en una VU sobre la capacidad de la VU para utilizar o no tarjetas de tacógrafo de generación 1 (anexo 1C, requisito 121).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Asignación de valor — Alineación de octeto: 'xxxxxxxa'B (8 bits)

Para la compatibilidad con la generación 1:

'a'B	Admisión de las tarjetas de tacógrafo de generación 1
	'0' B admite la generación 1,
	'1'B no admite la generación 1,
'xxxxxxx'B	RFU

2.170. **VuActivityDailyData**

Generación 1:

Información almacenada en una VU y relativa a los cambios de actividad y/o los cambios del régimen de conducción y/o los cambios del estado de la tarjeta que tengan lugar en un día civil determinado (anexo 1B, requisito 084) y a los estados de las ranuras a las 00.00 horas de ese día.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                  INTEGER SIZE(0..1440),
   activityChangeInfos                  SET SIZE(noOfActivityChanges) OF
                                        ActivityChangeInfo
}
```

noOfActivityChanges es el número de palabras de ActivityChangeInfo que hay en el conjunto activityChangeInfos.

activityChangeInfos es un conjunto de palabras de ActivityChangeInfo que se almacenan en la VU a lo largo del día Siempre incluye dos palabras de activityChangeInfo que dan el estado de las dos ranuras a las 00.00 horas de ese día.

2.171. **VuActivityDailyRecordArray**

Generación 2:

Información almacenada en una VU y relativa a los cambios de actividad y/o los cambios del régimen de conducción y/o los cambios del estado de la tarjeta que tengan lugar en un día civil determinado (anexo 1C, requisitos 105, 106 y 107) y a los estados de las ranuras a las 00.00 horas de ese día.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType denota el tipo de registro (ActivityChangeInfo). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de ActivityChangeInfo en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de palabras de ActivityChangeInfo que se almacenan en la VU a lo largo del día. Siempre incluye dos palabras de activityChangeInfo que dan el estado de las dos ranuras a las 00.00 horas de ese día.

2.172. **VuApprovalNumber**

Número de homologación de la unidad instalada en el vehículo.

Generación 1:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Asignación de valor: no especificado.

Generación 2:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

Asignación de valor:

el número de homologación deberá constar según haya sido publicado en el correspondiente sitio web de la Comisión Europea, es decir, por ejemplo, incluyendo guiones si los lleva. El número de homologación deberá estar alineado a la izquierda.

2.173. **VuCalibrationData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a los calibrados del aparato de control (anexo 1B, requisito 098).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords             INTEGER(0..255),
   vuCalibrationRecords                 SET SIZE(noOfVuCalibrationRecords) OF
                                        VuCalibrationRecord
}
```

noOfVuCalibrationRecords es el número de registros que hay en el conjunto vuCalibrationRecords.

vuCalibrationRecords es el conjunto de registros de calibrado.

2.174. **VuCalibrationRecord**

Información almacenada en una unidad instalada en el vehículo y relativa al calibrado del aparato de control (anexo 1B, requisito 098 y anexo 1C, requisitos 119 y 120).

Generación 1:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                   CalibrationPurpose,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber,
   workshopCardExpiryDate               TimeReal,
   vehicleIdentificationNumber          VehicleIdentificationNumber,
   vehicleRegistrationIdentification    VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant       W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment        K-ConstantOfRecordingEquipment,
   lTyreCircumference                   L-TyreCircumference,
   tyreSize                             TyreSize,
   authorisedSpeed                      SpeedAuthorised,
   oldOdometerValue                     OdometerShort,
   newOdometerValue                     OdometerShort,
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   nextCalibrationDate                  TimeReal
}
```

calibrationPurpose es el propósito del calibrado.

workshopName, workshopAddress son el nombre y la dirección del taller.

workshopCardNumber identifica la tarjeta de taller empleada durante el calibrado.

workshopCardExpiryDate es la fecha de expiración de la tarjeta.

vehicleIdentificationNumber es el VIN.

vehicleRegistrationIdentification contiene el VRN y el nombre del Estado miembro donde se matriculó el vehículo.

wVehicleCharacteristicConstant es el coeficiente característico del vehículo.

kConstantOfRecordingEquipment es la constante del aparato de control.

lTyreCircumference es la circunferencia efectiva de los neumáticos de las ruedas.

tyreSize son las dimensiones de las ruedas montadas en el vehículo.

authorisedSpeed es la velocidad autorizada del vehículo.

oldOdometerValue, newOdometerValue son la lectura anterior y la nueva lectura del cuentakilómetros.

oldTimeValue, newTimeValue son el valor anterior y el nuevo valor de la fecha y la hora.

nextCalibrationDate es la fecha del próximo calibrado del tipo especificado en CalibrationPurpose, a cargo de la autoridad de control autorizada.

Generación 2:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Además de los de la generación 1, se utiliza el siguiente elemento de datos:

sealDataVu da información sobre los precintos colocados en diversos componentes del vehículo.

2.175. **VuCalibrationRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a los calibrados del aparato de control (anexo 1C, requisitos 119 y 120).

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType denota el tipo de registro (VuCalibrationRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuCalibrationRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros de calibrado.

2.176. **VuCardIWData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a los ciclos de inserción y extracción de tarjetas de conductor o de taller en dicha unidad (anexo 1B, requisito 081, y anexo 1C, requisito 103).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords es el número de registros que hay en el conjunto vuCardIWRecords.

vuCardIWRecords es el conjunto de registros relativos a los ciclos de inserción y extracción de la tarjeta.

2.177. **VuCardIWRecord**

Información almacenada en una unidad instalada en el vehículo y relativa al ciclo de inserción y extracción de una tarjeta de conductor o de taller en dicha unidad (anexo 1B, requisito 081, y anexo 1C, requisito 102).

Generación 1:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName es el nombre y los apellidos del titular de la tarjeta de conductor o de taller, según los datos almacenados en la propia tarjeta.

fullCardNumber es el tipo de tarjeta, el nombre del Estado miembro que la expidió y el número de tarjeta, según los datos almacenados en la propia tarjeta.

cardExpiryDate es la fecha de expiración de la tarjeta, según los datos almacenados en la propia tarjeta.

cardInsertionTime es la fecha y la hora de inserción.

vehicleOdometerValueAtInsertion es la lectura del cuentakilómetros del vehículo en el momento de insertar la tarjeta.

cardSlotNumber es la ranura donde se inserta la tarjeta.

cardWithdrawalTime es la fecha y la hora de extracción.

vehicleOdometerValueAtWithdrawal es la lectura del cuentakilómetros del vehículo en el momento de extraer la tarjeta.

previousVehicleInfo contiene información sobre el vehículo anterior que utilizara el conductor, según los datos almacenados en la tarjeta.

manualInputFlag es una bandera que indica si el titular de la tarjeta ha introducido manualmente alguna actividad del conductor en el momento de insertar la tarjeta.

Generación 2:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                        HolderName,
   fullCardNumberAndGeneration           FullCardNumberAndGeneration,
   cardExpiryDate                        TimeReal,
   cardInsertionTime                     TimeReal,
   vehicleOdometerValueAtInsertion       OdometerShort,
   cardSlotNumber                        CardSlotNumber,
   cardWithdrawalTime                    TimeReal,
   vehicleOdometerValueAtWithdrawal      OdometerShort,
   previousVehicleInfo                   PreviousVehicleInfo,
   manualInputFlag                       ManualInputFlag
}
```

En lugar de fullCardNumber, la estructura de datos de la generación 2 utiliza el siguiente elemento de datos:

fullCardNumberAndGeneration es el tipo de tarjeta, el nombre del Estado miembro que la expidió, el número de tarjeta y su generación, según los datos almacenados en la propia tarjeta.

2.178. **VuCardIWRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a los ciclos de inserción y extracción de tarjetas de conductor o de taller en dicha unidad (anexo 1C, requisito 103).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType denota el tipo de registro (VuCardIWRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuCardIWRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros relativos a los ciclos de inserción y extracción de tarjetas.

2.179. **VuCardRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a una tarjeta de tacógrafo utilizada (anexo 1C, requisito 132).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber según se lee del archivo EF_ICC del MF de la tarjeta.

cardPersonaliserID según se lee del archivo EF_ICC del MF de la tarjeta.

typeOfTachographCardId según se lee del archivo EF_Application_Identification del DF_Tachograph_G2

cardStructureVersion según se lee del archivo EF_Application_Identification del DF_Tachograph_G2

cardNumber según se lee del archivo EF_Identification del DF_Tachograph_G2

2.180. **VuCardRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a las tarjetas de tacógrafo utilizadas con dicha unidad. Esta información se destina al análisis de los problemas VU — tarjeta (anexo 1C, requisito 132).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType denota el tipo de registro (VuCardRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuCardRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros relativos a las tarjetas de tacógrafo utilizadas con la VU.

2.181. **VuCertificate**

Certificado de la clave pública de una VU.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Generación 2:

El certificado de la VU más metadatos tal como se utilizan en el protocolo de transferencia.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType denota el tipo de registro (VuCertificate). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuCertificate en bytes.

noOfRecords es el número de registros que hay en el conjunto. El valor se pondrá a 1, ya que los certificados pueden tener diferentes longitudes.

records es un conjunto de certificados de VU.

2.183. **VuCompanyLocksData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a bloqueos introducidos por empresas (anexo 1B, requisito 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks es el número de bloqueos incluidos en vuCompanyLocksRecords.

vuCompanyLocksRecords es el conjunto de registros de bloqueos introducidos por empresas.

2.184. **VuCompanyLocksRecord**

Información almacenada en una unidad instalada en el vehículo y relativa a bloqueos introducidos por una empresa (anexo 1B, requisito 104, y anexo 1C, requisito 128).

Generación 1:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumber                  FullCardNumber
}
```

lockInTime, lockOutTime son la fecha y la hora de activación y desactivación del bloqueo.

companyName, companyAddress son el nombre y la dirección de la empresa relacionada con la activación del bloqueo.

companyCardNumber identifica la tarjeta empleada para la activación del bloqueo.

Generación 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

En lugar de companyCardNumber, la estructura de datos de la generación 2 utiliza el siguiente elemento de datos:

companyCardNumberAndGeneration identifica la tarjeta, incluida su generación, empleada para la activación del bloqueo.

2.185. **VuCompanyLocksRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a bloqueos introducidos por empresas (anexo 1C, requisito 128).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType denota el tipo de registro (VuCompanyLocksRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuCompanyLocksRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto. Valor 0..255.

records es el conjunto de registros de bloqueos introducidos por empresas.

2.186. **VuControlActivityData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a los controles efectuados con dicha unidad (anexo 1B, requisito 102).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls es el número de controles incluidos en vuControlActivityRecords.

vuControlActivityRecords es el conjunto de registros sobre actividades de control.

2.187. **VuControlActivityRecord**

Información almacenada en una unidad instalada en el vehículo y relativa a un control efectuado con dicha unidad (anexo 1B, requisito 102, y anexo 1C, requisito 126).

Generación 1:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType es el tipo de control.

controlTime es la fecha y la hora del control.

ControlCardNumber identifica la tarjeta de control empleada para el control.

downloadPeriodBeginTime es la hora de comienzo del período cuyos datos se transfieren, en caso de transferencia.

downloadPeriodEndTime es la hora de conclusión del período cuyos datos se transfieren, en caso de transferencia.

Generación 2:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

En lugar de controlCardNumber, la estructura de datos de la generación 2 utiliza el siguiente elemento de datos:

controlCardNumberAndGeneration identifica la tarjeta de control, incluida su generación, empleada para el control.

2.188. **VuControlActivityRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a los controles efectuados con dicha unidad (anexo 1C, requisito 126).

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuControlActivityRecord
}
```

recordType denota el tipo de registro (VuControlActivityRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuControlActivityRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros sobre actividades de control de la VU.

2.189. **VuDataBlockCounter**

Contador, almacenado en una tarjeta, que identifica secuencialmente los ciclos de inserción/extracción de la tarjeta en unidades instaladas en vehículos.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Asignación de valor: número consecutivo con un valor máximo de 9 999, y que vuelve a comenzar desde 0.

2.190. **VuDetailedSpeedBlock**

Información pormenorizada almacenada en una unidad instalada en el vehículo y relativa a la velocidad del vehículo durante un minuto en el que haya estado en movimiento (anexo 1B, requisito 093, y anexo 1C, requisito 116).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate es la fecha y la hora del primer valor de velocidad comprendido en ese bloque.

speedsPerSecond es la secuencia cronológica de las velocidades medidas cada segundo de ese minuto, empezando desde speedBlockBeginDate (inclusive).

2.191. **VuDetailedSpeedBlockRecordArray**

Generación 2:

Información pormenorizada almacenada en una unidad instalada en el vehículo y relativa a la velocidad del vehículo.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDetailedSpeedBlock
}
```

recordType denota el tipo de registro (VuDetailedSpeedBlock). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuDetailedSpeedBlock en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de bloques con datos pormenorizados sobre la velocidad.

2.192. **VuDetailedSpeedData**

Generación 1:

Información pormenorizada almacenada en una unidad instalada en el vehículo y relativa a la velocidad del vehículo.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks es el número de bloques con datos de velocidad que hay en el conjunto vuDetailedSpeed-Blocks.

vuDetailedSpeedBlocks es el conjunto de bloques con datos pormenorizados sobre la velocidad.

2.193. **VuDownloadablePeriod**

La fecha más antigua y la más reciente para las que una unidad instalada en el vehículo conserva datos relativos a las actividades de los conductores (anexo 1B, requisitos 081, 084 o 087, y anexo 1C, requisitos 102, 105 y 108).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime es la fecha y la hora más antiguas en que se insertó una tarjeta, ocurrió un cambio de actividad o se introdujo un lugar; según los datos almacenados en la VU.

maxDownloadableTime es la fecha y la hora más recientes en que se insertó una tarjeta, ocurrió un cambio de actividad o se introdujo un lugar; según los datos almacenados en la VU.

2.194. **VuDownloadablePeriodRecordArray**

Generación 2:

El VUDownloadablePeriod más metadatos tal como se utilizan en el protocolo de transferencia.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuDownloadablePeriod
}
```

recordType denota el tipo de registro (VuDownloadablePeriod). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuDownloadablePeriod en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros de VuDownloadablePeriod.

2.195. **VuDownloadActivityData**

Información almacenada en una unidad instalada en el vehículo y relativa a su última transferencia (anexo 1B, requisito 105, y anexo 1C, requisito 129).

Generación 1:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumber                      FullCardNumber,
   companyOrWorkshopName               Name
}
```

downloadingTime es la fecha y la hora de la transferencia.

fullCardNumber identifica la tarjeta empleada para autorizar la transferencia.

companyOrWorkshopName es el nombre de la empresa o del centro de ensayo.

Generación 2:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

En lugar de fullCardNumber, la estructura de datos de la generación 2 utiliza el siguiente elemento de datos:

fullCardNumberAndGeneration identifica la tarjeta, incluida su generación, empleada para autorizar la transferencia.

2.196. **VuDownloadActivityDataRecordArray**

Generación 2:

Información relativa a la última transferencia de la VU (anexo 1C, requisito 129).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType denota el tipo de registro (VuDownloadActivityData). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuDownloadActivityData en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros de datos sobre actividades de transferencia.

2.197. **VuEventData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes (anexo 1B, requisito 094, salvo el incidente de exceso de velocidad).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents es el número de incidentes incluidos en el conjunto vuEventRecords.

vuEventRecords es un conjunto de registros sobre incidentes.

2.198. **VuEventRecord**

Información almacenada en una unidad instalada en el vehículo y relativa a un incidente (anexo 1B, requisito 094 y anexo 1C, requisito 117, salvo el incidente de exceso de velocidad).

Generación 1:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType es el tipo de incidente.

eventRecordPurpose es el propósito con que se ha registrado ese incidente.

eventBeginTime es la fecha y la hora de comienzo del incidente.

eventEndTime es la fecha y la hora en que termina el incidente.

cardNumberDriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que comenzó el incidente.

cardNumberCodriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del segundo conductor en el momento en que comenzó el incidente.

cardNumberDriverSlotEnd identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que finalizó el incidente.

cardNumberCodriverSlotEnd identifica la tarjeta que estaba insertada en la ranura del segundo conductor en el momento en que finalizó el incidente.

similarEventsNumber es el número de incidentes similares ocurridos ese día.

Esta secuencia puede utilizarse para todos los incidentes, excepto los de exceso de velocidad.

Generación 2:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Además de los de la generación 1, se utilizan los siguientes elementos de datos:

manufacturerSpecificEventFaultData contiene información adicional sobre el incidente, específica del fabricante.

En lugar de cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd y cardNumberCodriverSlotEnd, la estructura de datos de la generación 2 utiliza los siguientes elementos de datos:

cardNumberAndGenDriverSlotBegin identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del conductor en el momento en que comenzó el incidente.

cardNumberAndGenCodriverSlotBegin identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del segundo conductor en el momento en que comenzó el incidente.

cardNumberAndGenDriverSlotEnd identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del conductor en el momento en que terminó el incidente.

cardNumberAndGenCodriverSlotEnd identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del segundo conductor en el momento en que terminó el incidente.

Si el incidente es un conflicto temporal, eventBeginTime y eventEndTime deben interpretarse como sigue:

eventBeginTime es la fecha y la hora del aparato de control.

eventEndTime es la fecha y la hora GNSS.

2.199. **VuEventRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes (anexo 1C, requisito 117, salvo el incidente de exceso de velocidad).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType denota el tipo de registro (VuEventRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuEventRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros sobre incidentes.

2.200. **VuFaultData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a fallos (anexo 1B, requisito 096).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults es el número de fallos incluidos en el conjunto vuFaultRecords.

vuFaultRecords es un conjunto de registros sobre fallos.

2.201. **VuFaultRecord**

Información almacenada en una unidad instalada en el vehículo y relativa a un fallo (anexo 1B, requisito 096, y anexo 1C, requisito 118).

Generación 1:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType es el tipo de fallo del aparato de control.

faultRecordPurpose es el propósito con que se ha registrado ese fallo.

faultBeginTime es la fecha y la hora de comienzo del fallo.

faultEndTime es la fecha y la hora en que termina el fallo.

cardNumberDriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que comenzó el fallo.

cardNumberCodriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del segundo conductor en el momento en que comenzó el fallo.

cardNumberDriverSlotEnd identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que terminó el fallo.

cardNumberCodriverSlotEnd identifica la tarjeta que estaba insertada en la ranura del segundo conductor en el momento en que terminó el fallo.

Generación 2:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Además de los de la generación 1, se utiliza el siguiente elemento de datos:

manufacturerSpecificEventFaultData contiene información adicional sobre el fallo, específica del fabricante.

En lugar de cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd y cardNumberCodriverSlotEnd, la estructura de datos de la generación 2 utiliza los siguientes elementos de datos:

cardNumberAndGenDriverSlotBegin identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del conductor en el momento en que comenzó el fallo.

cardNumberAndGenCodriverSlotBegin identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del segundo conductor en el momento en que comenzó el fallo.

cardNumberAndGenDriverSlotEnd identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del conductor en el momento en que terminó el fallo.

cardNumberAndGenCodriverSlotEnd identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del segundo conductor en el momento en que terminó el fallo.

2.202. **VuFaultRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a fallos (anexo 1B, requisito 118).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType denota el tipo de registro (VuFaultRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuFaultRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros sobre fallos.

2.203. **VuGNSSCDRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a la posición GNSS del vehículo si el tiempo de conducción continua del conductor alcanza un múltiplo de tres horas (anexo 1C, requisitos 108 y 110).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp es la fecha y hora en las que el tiempo de conducción continua del titular de la tarjeta llega a un múltiplo de tres horas.

cardNumberAndGenDriverSlot identifica la tarjeta, incluida su generación, que está insertada en la ranura del conductor.

cardNumberAndGenCodriverSlot identifica la tarjeta, incluida su generación, que está insertada en la ranura del segundo conductor.

gnssPlaceRecord contiene información relacionada con la posición del vehículo.

2.204. **VuGNSSCDRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a la posición GNSS del vehículo si el tiempo de conducción continua del conductor alcanza un múltiplo de tres horas (anexo 1C, requisitos 108 y 110).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType denota el tipo de registro (VuGNSSCDRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuGNSSCDRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros GNSS sobre conducción continua.

2.205. **VuIdentification**

Información almacenada en una unidad instalada en el vehículo y relativa a la identificación de dicha unidad (anexo 1B, requisito 075 y anexo 1C, requisitos 93 y 121).

Generación 1:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                     VuManufacturerName,
   vuManufacturerAddress                  VuManufacturerAddress,
   vuPartNumber                           VuPartNumber,
   vuSerialNumber                         VuSerialNumber,
   vuSoftwareIdentification               VuSoftwareIdentification,
   vuManufacturingDate                    VuManufacturingDate,
   vuApprovalNumber                       VuApprovalNumber
}
```

vuManufacturerName es el nombre del fabricante de la VU.

vuManufacturerAddress es la dirección del fabricante de la VU.

vuPartNumber es el número de pieza de la VU.

vuSerialNumber es el número de serie de la VU.

vuSoftwareIdentification identifica el *software* instalado en la VU.

vuManufacturingDate es la fecha de fabricación de la VU.

vuApprovalNumber es el número de homologación de la VU.

Generación 2:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

Además de los de la generación 1, se utiliza el siguiente elemento de datos:

vuGeneration indica la generación de la VU.

vuAbility aporta información sobre si la VU soporta o no las tarjetas de tacógrafo de la generación 1.

2.206. **VuIdentificationRecordArray**

Generación 2:

El VuIdentification más metadatos tal como se utilizan en el protocolo de transferencia.

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType denota el tipo de registro (VuIdentification). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuIdentification en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros VuIdentification.

2.207. **VuITSConsentRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a la autorización de un conductor en relación con la utilización de sistemas de transporte inteligentes.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identifica la tarjeta, incluida su generación. Debe ser una tarjeta de conductor o de taller.

consent es una bandera que indica si el conductor ha dado su consentimiento en relación con el uso de sistemas de transporte inteligentes con este vehículo/unidad instalada en el vehículo.

Asignación de valor:

TRUE indica el consentimiento del conductor en relación con el uso de sistemas de transporte inteligentes

FALSE indica la negativa del conductor en relación con el uso de sistemas de transporte inteligentes

2.208. **VuITSConsentRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa al consentimiento del conductor en relación con el uso de sistemas de transporte inteligentes (anexo 1C, requisito 200).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType denota el tipo de registro (VuITSConsentRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuITSConsentRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros de consentimiento en relación con el ITS.

2.209. **VuManufacturerAddress**

Dirección del fabricante de la unidad instalada en el vehículo.

```
VuManufacturerAddress ::= Address
```

Asignación de valor: no especificado.

2.210. **VuManufacturerName**

Nombre del fabricante de la unidad instalada en el vehículo.

```
VuManufacturerName ::= Name
```

Asignación de valor: no especificado.

2.211. **VuManufacturingDate**

Fecha de fabricación de la unidad instalada en el vehículo.

```
VuManufacturingDate ::= TimeReal
```

Asignación de valor: no especificado.

2.212. **VuOverSpeedingControlData**

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes de exceso de velocidad ocurridos desde el último control del exceso de velocidad (anexo 1B, requisito 095, y anexo 1C, requisito 117).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime            TimeReal,
   firstOverspeedSince                 TimeReal,
   numberOfOverspeedSince              OverspeedNumber
}
```

lastOverspeedControlTime es la fecha y la hora del último control del exceso de velocidad.

firstOverspeedSince es la fecha y la hora del primer exceso de velocidad ocurrido tras este control.

numberOfOverspeedSince es el número de incidentes de exceso de velocidad ocurridos después del último control del exceso de velocidad.

2.213. **VuOverSpeedingControlDataRecordArray**

Generación 2:

El VuOverSpeedingControlData más metadatos tal como se utilizan en el protocolo de transferencia.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuOverSpeedingControlData
}
```

recordType denota el tipo de registro (VuOverSpeedingControlData). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuOverSpeedingControlData en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros de datos de controles de exceso de velocidad.

2.214. **VuOverSpeedingEventData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes de exceso de velocidad (anexo 1B, requisito 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents            INTEGER(0..255),
   vuOverSpeedingEventRecords          SET SIZE(noOfVuOverSpeedingEvents) OF
                                       VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents es el número de incidentes incluidos en el conjunto vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords es un conjunto de registros sobre incidentes de exceso de velocidad.

2.215. **VuOverSpeedingEventRecord**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes de exceso de velocidad (anexo 1B, requisito 094, y anexo 1C, requisito 117).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberDriverSlotBegin          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType es el tipo de incidente.

eventRecordPurpose es el propósito con que se ha registrado ese incidente.

eventBeginTime es la fecha y la hora de comienzo del incidente.

eventEndTime es la fecha y la hora en que termina el incidente.

maxSpeedValue es la velocidad máxima medida durante el incidente.

averageSpeedValue es la media aritmética de las velocidades medidas durante el incidente.

cardNumberDriverSlotBegin identifica la tarjeta que estaba insertada en la ranura del conductor en el momento en que comenzó el incidente.

similarEventsNumber es el número de incidentes similares ocurridos ese día.

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes de exceso de velocidad (anexo 1B, requisito 094, y anexo 1C, requisito 117).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

En lugar de cardNumberDriverSlotBegin, la estructura de datos de la generación 2 utiliza el siguiente elemento de datos:

cardNumberAndGenDriverSlotBegin identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del conductor en el momento en que comenzó el incidente.

2.216. **VuOverSpeedingEventRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes de exceso de velocidad (anexo 1C, requisito 117).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuOverSpeedingEventRecord
}
```

recordType denota el tipo de registro (VuOverSpeedingEventRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuOverSpeedingEventRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros sobre incidentes de exceso de velocidad.

2.217. **VuPartNumber**

Número de pieza de la unidad instalada en el vehículo.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Asignación de valor: específica del fabricante de la VU.

2.218. **VuPlaceDailyWorkPeriodData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a los lugares donde los conductores comienzan o terminan un período de trabajo diario (anexo 1B, requisito 087, y anexo 1C, requisitos 108 y 110).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords es el número de registros incluidos en el conjunto vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords es un conjunto de registros relativos a lugares.

2.219. **VuPlaceDailyWorkPeriodRecord**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a un lugar donde un conductor comienza o termina un período de trabajo diario (anexo 1B, requisito 087, y anexo 1C, requisitos 108 y 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber es el tipo de tarjeta de conductor, el Estado miembro que la ha expedido y el número de tarjeta.

placeRecord contiene la información relativa al lugar introducido.

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a un lugar donde un conductor comienza o termina un período de trabajo diario (anexo 1B, requisito 087, y anexo 1C, requisitos 108 y 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

En lugar de fullCardNumber, la estructura de datos de la generación 2 utiliza el siguiente elemento de datos:

fullCardNumberAndGeneration es el tipo de tarjeta, el nombre del Estado miembro que la expidió, el número de tarjeta y su generación, según los datos almacenados en la propia tarjeta.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a los lugares donde los conductores comienzan o terminan un período de trabajo diario (anexo 1C, requisitos 108 y 110).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType denota el tipo de registro (VuPlaceDailyWorkPeriodRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuPlaceDailyWorkPeriodRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es el conjunto de registros relativos a lugares.

2.221. **VuPrivateKey**

Generación 1:

La clave privada de una unidad instalada en el vehículo.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Generación 1:

La clave pública de una unidad instalada en el vehículo.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Número de serie de la unidad instalada en el vehículo (anexo 1B, requisito 075, y anexo 1C, requisito 93).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Fecha de instalación de la versión de *software* que lleva la unidad instalada en el vehículo.

```
VuSoftInstallationDate ::= TimeReal
```

Asignación de valor: no especificado.

2.225. **VuSoftwareIdentification**

Información almacenada en una unidad instalada en el vehículo y relativa al *software* instalado.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion es el número de la versión de *software* que lleva la VU.

vuSoftInstallationDate es la fecha de instalación de la versión de *software*.

2.226. **VuSoftwareVersion**

Número de la versión de *software* que lleva la VU.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Asignación de valor: no especificado.

2.227. **VuSpecificConditionData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a condiciones específicas.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords es el número de registros incluidos en el conjunto specificConditionRecords.

specificConditionRecords es el conjunto de registros relativos a condiciones específicas.

2.228. **VuSpecificConditionRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a condiciones específicas (anexo 1C, requisito 130).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType denota el tipo de registro (SpecificConditionRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de SpecificConditionRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros relativos a condiciones específicas.

2.229. **VuTimeAdjustmentData**

Generación 1:

Información almacenada en una unidad instalada en el vehículo y relativa a los ajustes de la hora que se han efectuado fuera del marco de un calibrado regular (anexo 1B, requisito 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                INTEGER(0..6),
   vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                       VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords es el número de registros que hay en el conjunto vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords es un conjunto de registros sobre ajustes de la hora.

2.230. **VuTimeAdjustmentGNSSRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a un ajuste de la hora basado en datos horarios procedentes del GNSS (anexo 1C, requisitos 124 y 125).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue son el valor anterior y el nuevo valor de la fecha y la hora.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a un ajuste de la hora realizado con datos horarios procedentes del GNSS (anexo 1C, requisitos 124 y 125).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuTimeAdjustmentGNSSRecord
}
```

recordType denota el tipo de registro (VuTimeAdjustmentGNSSRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuTimeAdjustmentGNSSRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros de ajuste de la hora basado en el GNSS.

2.232. **VuTimeAdjustmentRecord**

Información almacenada en una unidad instalada en el vehículo y relativa a un ajuste de la hora efectuado fuera del marco de un calibrado regular (anexo 1B, requisito 101, y anexo 1C, requisitos 124 y 125).

Generación 1:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue son el valor anterior y el nuevo valor de la fecha y la hora.

workshopName, workshopAddress son el nombre y la dirección del taller.

workshopCardNumber identifica la tarjeta de taller empleada para realizar el ajuste de la hora.

Generación 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

En lugar de workshopCardNumber, la estructura de datos de la generación 2 utiliza el siguiente elemento de datos:

workshopCardNumberAndGeneration identifica la tarjeta de taller, incluida su generación, empleada para realizar el ajuste de la hora.

2.233. **VuTimeAdjustmentRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a ajustes de la hora que se han efectuado fuera del marco de un calibrado regular (anexo 1C, requisitos 124 y 125).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType denota el tipo de registro (VuTimeAdjustmentRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuTimeAdjustmentRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros de ajuste de la hora.

2.234. **WorkshopCardApplicationIdentification**

Información almacenada en una tarjeta de taller y relativa a la identificación de la aplicación de la tarjeta (anexo 1C, requisitos 307 y 330).

Generación 1:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId especifica el tipo de tarjeta utilizado.

cardStructureVersion especifica la versión de la estructura que se utiliza en la tarjeta.

noOfEventsPerType es el número de incidentes de cada tipo que puede registrar la tarjeta.

noOfFaultsPerType es el número de fallos de cada tipo que puede registrar la tarjeta.

activityStructureLength indica el número de bytes disponibles para almacenar registros de actividad.

noOfCardVehicleRecords es el número de registros del vehículo que caben en la tarjeta.

noOfCardPlaceRecords es el número de lugares que puede registrar la tarjeta.

noOfCalibrationRecords es el número de registros de calibrado que puede almacenar la tarjeta.

Generación 2:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Además de los de la generación 1, se utilizan los siguientes elementos de datos:

noOfGNSSCDRecords es el número de registros GNSS de conducción continua que puede almacenar la tarjeta.

noOfSpecificConditionRecords es el número de registros de condiciones específicas que puede almacenar la tarjeta.

2.235. **WorkshopCardCalibrationData**

Información almacenada en una tarjeta de taller y relativa a las actividades del taller realizadas con dicha tarjeta (anexo 1C, requisitos 314, 316, 337 y 339).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber es el número total de calibrados realizados con la tarjeta.

calibrationPointerNewestRecord es el índice del último registro de calibrado actualizado.

Asignación de valor: número correspondiente al numerador del registro de calibrado. Al primer registro de la estructura se le asigna el número '0'.

calibrationRecords es el conjunto de registros que contienen información sobre calibrados y/o ajustes de la hora.

2.236. **WorkshopCardCalibrationRecord**

Información almacenada en una tarjeta de taller y relativa a un calibrado realizado con la tarjeta (anexo 1C, requisitos 314 y 337).

Generación 1:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose es el propósito del calibrado.

vehicleIdentificationNumber es el VIN.

vehicleRegistration contiene el VRN y el nombre del Estado miembro donde se matriculó el vehículo.

wVehicleCharacteristicConstant es el coeficiente característico del vehículo.

kConstantOfRecordingEquipment es la constante del aparato de control.

lTyreCircumference es la circunferencia efectiva de los neumáticos de las ruedas.

tyreSize son las dimensiones de las ruedas montadas en el vehículo.

authorisedSpeed es la velocidad máxima autorizada del vehículo.

oldOdometerValue, newOdometerValue son la lectura anterior y la nueva lectura del cuentakilómetros.

oldTimeValue, newTimeValue son el valor anterior y el nuevo valor de la fecha y la hora.

nextCalibrationDate es la fecha del próximo calibrado del tipo especificado en CalibrationPurpose, a cargo de la autoridad de control autorizada.

vuPartNumber, **vuSerialNumber** y **sensorSerialNumber** son los elementos de datos para la identificación del aparato de control.

Generación 2:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Además de los de la generación 1, se utilizan los siguientes elementos de datos:

sensorGNSSSerialNumber que identifica un dispositivo GNSS externo.

rcmSerialNumber que identifica un módulo de comunicación a distancia.

sealDataCard da información sobre los precintos colocados en diversos componentes del vehículo.

2.237. **WorkshopCardHolderIdentification**

Información almacenada en una tarjeta de taller y relativa a la identificación del titular de la tarjeta (anexo 1C, requisitos 311 y 334).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName es el nombre del taller que corresponde al titular de la tarjeta.

workshopAddress es la dirección del taller que corresponde al titular de la tarjeta.

cardHolderName es el nombre y los apellidos del titular (por ejemplo, el nombre del mecánico).

cardHolderPreferredLanguage es el idioma preferido por el titular de la tarjeta.

2.238. **WorkshopCardPIN**

Número de identificación personal de la tarjeta de taller (anexo 1C. requisitos 309 y 332).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Asignación de valor: el PIN que conoce el titular de la tarjeta, rellenado por la derecha con bytes 'FF' hasta llegar a 8 bytes.

2.239. **W-VehicleCharacteristicConstant**

Coeficiente característico del vehículo [definición k)].

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Asignación de valor: impulsos por kilómetro en el intervalo operativo de 0 a 64 255 impulsos/km.

2.240. **VuPowerSupplyInterruptionRecord**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes de interrupción del suministro eléctrico (anexo 1C, requisito 117).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType es el tipo de incidente.

eventRecordPurpose es el propósito con que se ha registrado ese incidente.

eventBeginTime es la fecha y la hora de comienzo del incidente.

eventEndTime es la fecha y la hora en que termina el incidente.

cardNumberAndGenDriverSlotBegin identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del conductor en el momento en que comenzó el incidente.

cardNumberAndGenDriverSlotEnd identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del conductor en el momento en que terminó el incidente.

cardNumberAndGenCodriverSlotBegin identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del segundo conductor en el momento en que comenzó el incidente.

cardNumberAndGenCodriverSlotEnd identifica la tarjeta, incluida su generación, que estaba insertada en la ranura del segundo conductor en el momento en que terminó el incidente.

similarEventsNumber es el número de incidentes similares ocurridos ese día.

2.241. **VuPowerSupplyInterruptionRecordArray**

Generación 2:

Información almacenada en una unidad instalada en el vehículo y relativa a incidentes de interrupción del suministro eléctrico (anexo 1C, requisito 117).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType denota el tipo de registro (VuPowerSupplyInterruptionRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de VuPowerSupplyInterruptionRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros sobre incidentes de interrupción del suministro eléctrico.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Generación 2:

Conjunto de SensorExternalGNSSCoupledRecord más metadatos tal y como se utiliza en el protocolo de transferencia.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType denota el tipo de registro (SensorExternalGNSSCoupledRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de SensorExternalGNSSCoupledRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros de SensorExternalGNSSCoupled.

2.243. **VuSensorPairedRecordArray**

Generación 2:

Conjunto de SensorPairedRecord más metadatos tal y como se utiliza en el protocolo de transferencia.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType denota el tipo de registro (SensorPairedRecord). **Asignación de valor**: véase RecordType.

recordSize es el tamaño de SensorPairedRecord en bytes.

noOfRecords es el número de registros que hay en el conjunto.

records es un conjunto de registros de acoplamiento de sensor.

3. DEFINICIONES DE LOS INTERVALOS DE VALORES Y TAMAÑOS ADMISIBLES

Definición de valores variables empleados en las definiciones del apartado 2.

```
TimeRealRange ::= 2^32-1
```

4. JUEGOS DE CARACTERES

Las cadenas IA5 utilizan los caracteres ASCII que se definen en la norma ISO/CEI 8824-1. Para facilitar la lectura y las referencias, a continuación se ofrece la asignación de valores. La norma ISO/CEI 8824-1 prevalece sobre esta nota informativa en caso de discrepancia.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Otras cadenas de caracteres (Address, Name, VehicleRegistrationNumber) utilizan, asimismo, los caracteres del código de caracteres decimales 161 a 255 del código estándar de 8 bits siguiente, especificados por el número de página de código: Conjunto de caracteres estándar	Página de código (Decimal)
ISO/CEI 8859-1 Latín-1, Europa Occidental	1
ISO/CEI 8859-2 Latín-2, Europa Central	2
ISO/CEI 8859-3 Latín-3, Europa Meridional	3
ISO/CEI 8859-5 Latín / Cirílico	5
ISO/CEI 8859-7 Latín / Griego	7
ISO/CEI 8859-9 Latín-5 / Turco	9
ISO/CEI 8859-13 Latín-7 / Países Bálticos	13
ISO/CEI 8859-15 Latín-9	15
ISO/CEI 8859-16 Latín-10, Europa Sudoriental	16
KOI8-R Latín / Cirílico	80
KOI8-U Latín / Cirílico	85

5. CODIFICACIÓN

Si se aplican las reglas de codificación NSA.1, todos los tipos de datos definidos deberán codificarse con arreglo a la norma ISO/CEI 8825-2, variante alineada.

6. IDENTIFICADORES DE OBJETO E IDENTIFICADORES DE APLICACIÓN

6.1. **Identificadores de objeto**

Los identificadores de objeto (OID) que figuran en el presente capítulo solo son pertinentes para la generación 2. Estos OID se especifican en TR-03110-3 y se repiten aquí en aras de la exhaustividad. Estos OID están contenidos en el subárbol de bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identificadores del protocolo de autenticación de la VU

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                 OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Ejemplo: Supongamos que la autenticación de la VU debe hacerse con SHA- 384; en tal caso, se utilizará el identificador de objeto (en notación ASN.1) `bsi-de protocols(2) smartcard(2) 2 2 4`. El valor de este identificador de objeto en notación de puntos es `0.4.0.127.0.7.2.2.2.2.4`.

	Notación de puntos	Notación de bytes
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	'04 00 7F 00 07 02 02 02 02 03'
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	'04 00 7F 00 07 02 02 02 02 04'
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	'04 00 7F 00 07 02 02 02 02 05'

Identificadores del protocolo de autenticación del chip

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Ejemplo: Supongamos que la autenticación del chip se hará utilizando el algoritmo ECDH, que da lugar a una longitud de clave de sesión AES de 128 bits. Esta clave de sesión se utilizará luego en el modo de funcionamiento CBC para garantizar la confidencialidad de los datos y con el algoritmo CMAC para garantizar la autenticidad de los datos. Por consiguiente, el identificador de objeto que hay que usar es (en notación ASN.1) `bsi-de protocols(2) smartcard(2) 3 2 2`. El valor de este identificador de objeto en notación de puntos es `0.4.0.127.0.7.2.2.3.2.2`.

	Notación de puntos	Notación de bytes
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	'04 00 7F 00 07 02 02 03 02 02'
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	'04 00 7F 00 07 02 02 03 02 03'
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	'04 00 7F 00 07 02 02 03 02 04'

6.2. **Identificadores de aplicación**

Generación 2:

El identificador de aplicación (AID) para el dispositivo GNSS externo (generación 2) viene dado por 'FF 44 54 45 47 4D'. Se trata de un AID propio con arreglo a la norma ISO/CEI 7816-4.

Nota: Los últimos 5 bytes codifican DTEGM para el dispositivo GNSS externo del tacógrafo.

El identificador de aplicación para la aplicación de la tarjeta de tacógrafo de generación 2 viene dado por 'FF 53 4D 52 44 54'. Se trata de un AID propio con arreglo a la norma ISO/CEI 7816-4.

Apéndice 2

ESPECIFICACIONES DE LAS TARJETAS DE TACÓGRAFO

ÍNDICE

1. INTRODUCCIÓN

1.1. **Abreviaciones**

A efectos del presente apéndice se utilizan las siguientes siglas:

AC	Condiciones de acceso
AES	Norma de cifrado avanzado
AID	Identificador de aplicación
ALW	Siempre
APDU	Unidad de datos de protocolo de una aplicación (estructura de un comando)
ATR	Respuesta a reinicio
AUT	Autentificado
C6, C7	Contactos n.º 6 y 7 de la tarjeta, tal y como se describen en la norma ISO/CEI 7816-2
cc	Ciclos de reloj
CHV	Información para la verificación del titular de la tarjeta
CLA	Byte de clase de un comando APDU
DSRC	Comunicación especializada de corto alcance
DF	Archivo dedicado. Un DF puede contener otros archivos (EF o DF)
ECC	Criptografía de curva elíptica
EF	Archivo elemental
etu	Unidad de tiempo elemental
G1	Generación 1
G2	Generación 2
IC	Circuito integrado
ICC	Tarjeta de circuito integrado
ID	Identificador
IFD	Dispositivo de interfaz
IFS	Tamaño del campo de información
IFSC	Tamaño del campo de información para la tarjeta

IFSD	Dispositivo de tamaño del campo de información (para el terminal)
INS	Byte de instrucción de un comando APDU
Lc	Longitud de los datos de entrada para un comando APDU
Le	Longitud de los datos esperados (datos de salida para un comando)
MF	Archivo principal (DF raíz)
NAD	Dirección de nodo empleada en el protocolo T=1
NEV	Nunca
P1-P2	Bytes de parámetros
PIN	Número de identificación personal
PRO SM	Protegido con mensajería segura
PTS	Selección de la transmisión de protocolo
RFU	Reservado para uso futuro
RST	Reinicio (de la tarjeta)
SFID	Identificador EF corto
SM	Mensajería segura
SW1-SW2	Bytes de estado
TS	Carácter ATR inicial
VPP	Tensión de programación
VU	Unidad instalada en el vehículo
XXh	Valor XX en notación hexadecimal
'XXh'	Valor XX en notación hexadecimal
||	Símbolo de concatenación 03||04=0304

1.2. **Referencias**

En el presente apéndice se utilizan las referencias siguientes:

ISO/CEI 7816-2 Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) — Parte 2: Dimensiones y ubicación de los contactos. ISO/CEI 7816-2:2007.

ISO/CEI 7816-3 Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) — Parte 3: Interfaz eléctrica y protocolos de transmisión. ISO/CEI 7816-3:2006.

ISO/CEI 7816-4 Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) — Parte 4: Organización, seguridad y comandos para intercambio. ISO/CEI 7816-4:2013 + Cor 1: 2014.

ISO/CEI 7816-6 Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) — Parte 6: Elementos de datos interindustriales para intercambio. ISO/CEI 7816-6:2004 + Cor 1: 2006.

ISO/CEI 7816-8 Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) — Parte 8: Comandos para operaciones de seguridad. ISO/CEI 7816-8:2004.

ISO/CEI 9797-2 Tecnología de la información — Técnicas de seguridad — Códigos de autenticación de mensajes (MACs) — Parte 2: Mecanismos que utilizan una función específica de comprobación aleatoria. ISO/CEI 9797-2:2011

2. CARACTERÍSTICAS ELÉCTRICAS Y FÍSICAS

TCS_01 Todas las señales electrónicas deberán ser conformes a la norma ISO/CEI 7816-3, a menos que se especifique otra cosa.

TCS_02 La ubicación y dimensiones de los contactos de las tarjetas se ajustarán a lo dispuesto en la norma ISO/CEI 7816-2.

2.1. **Tensión de alimentación y consumo de corriente**

TCS_03 La tarjeta deberá trabajar con arreglo a las especificaciones, dentro de los límites de consumo especificados en la norma ISO/CEI 7816-3.

TCS_04 La tarjeta debe funcionar con Vcc = 3V (± 0,3 V) o con Vcc = 5V (± 0,5 V).

La tensión deberá seleccionarse con arreglo a lo dispuesto en la norma ISO/CEI 7816-3.

2.2. **Tensión de programación V_{pp}**

TCS_05 La tarjeta no debe requerir tensión de programación en la patilla C6. Se espera que la patilla C6 no esté conectada a un IFD. El contacto C6 podrá estar conectado a la tensión V_{cc} de la tarjeta, pero no a masa. Dicha tensión no deberá interpretarse en ningún caso.

2.3. **Generación y frecuencia del reloj**

TCS_06 La tarjeta deberá funcionar en el intervalo de frecuencias de 1 a 5 MHz y debe admitir frecuencias mayores. La frecuencia del reloj podrá experimentar una variación del ± 2 % dentro de una sesión de la tarjeta. La frecuencia del reloj la genera la Unidad instalada en el vehículo (VU) y no la propia tarjeta. El ciclo de trabajo puede variar entre el 40 % y el 60 %.

TCS_07 El reloj externo puede ser detenido en las condiciones que especifica el archivo EF ICC de la tarjeta. El primer byte del cuerpo del archivo EF ICC codifica las condiciones del modo clockstop:

Bajo	Alto		
Bit 3	Bit 2	Bit 1	
0	0	1	Se permite clockstop, no hay un nivel preferido
0	1	1	Se permite clockstop, preferiblemente en el nivel alto
1	0	1	Se permite clockstop, preferiblemente en el nivel bajo
0	0	0	No se permite clockstop
0	1	0	Se permite clockstop exclusivamente en el nivel alto
1	0	0	Se permite clockstop exclusivamente en el nivel bajo

Los bits 4 a 8 no se utilizan.

2.4. **Contacto de entrada/salida**

TCS_08 El contacto C7 de entrada/salida sirve para recibir y transmitir datos al IFD. Durante el funcionamiento de dicho contacto, tan solo podrán estar en modo de transmisión la tarjeta o el IFD. Si ambas unidades estuvieran en el modo de transmisión, la tarjeta no deberá sufrir daños. A menos que se esté transmitiendo, la tarjeta deberá entrar en el modo de recepción.

2.5. **Estados de la tarjeta**

TCS_09 La tarjeta trabaja en dos estados mientras se aplica la tensión de alimentación:

en estado de funcionamiento mientras se ejecutan los comandos o se mantiene la interconexión con la unidad digital,

en estado de reposo en el resto de casos; en este estado la tarjeta deberá retener todos los datos.

3. SOPORTE FÍSICO Y COMUNICACIONES

3.1. **Introducción**

El presente apartado describe la funcionalidad mínima que precisan las tarjetas de tacógrafo y las VU para garantizar un correcto funcionamiento e interoperabilidad.

Las tarjetas de tacógrafo cumplen en todo lo posible las normas ISO/CEI aplicables (en especial la norma ISO/CEI 7816). No obstante, a continuación se ofrece una descripción completa de los comandos y protocolos a fin de especificar algunos casos de uso restringido o determinadas diferencias que puedan existir. Los comandos especificados son totalmente conformes a las normas citadas, salvo en los casos que se indican.

3.2. **Protocolo de transmisión**

TCS_10 El protocolo de transmisión deberá ser conforme a la norma ISO/CEI 7816-3 para T = 0 y T = 1. En particular, la VU deberá reconocer las extensiones de tiempo de espera que envíe la tarjeta.

3.2.1 *Protocolos*

TCS_11 La tarjeta deberá ofrecer los protocolos **T = 0** y **T = 1**. Además, la tarjeta podrá admitir otros protocolos orientados a la conexión.

TCS_12 **T = 0** es el protocolo por defecto, de modo que se precisa un comando **PTS** para cambiar al protocolo **T = 1**.

TCS_13 Los dispositivos deberán admitir la **convención directa** en ambos protocolos: por consiguiente, la convención directa es obligatoria para la tarjeta.

TCS_14 El byte correspondiente al **tamaño del campo de información de la tarjeta** en la ATR deberá presentarse en el carácter TA3. Este valor deberá ser al menos 'F0h' (= 240 bytes).

Los protocolos estarán sujetos a las restricciones siguientes:

TCS_15 **T=0**

— El dispositivo de interfaz deberá admitir una respuesta en la entrada/salida después del flanco ascendente de la señal en RST a partir de 400 cc.

— El dispositivo de interfaz deberá ser capaz de leer caracteres separados por 12 etu.

— El dispositivo de interfaz deberá leer un carácter erróneo y su repetición cuando estén separados por 13 etu. Si se detecta un carácter erróneo, la señal de error en la entrada/salida puede ocurrir entre 1 etu y 2 etu más tarde. El dispositivo deberá admitir un retardo de 1 etu.

— El dispositivo de interfaz deberá aceptar una respuesta ATR de 33 bytes (TS+32).

— Si TC1 está presente en la respuesta ATR, el Extra Guard Time deberá estar presente para los caracteres que envíe el dispositivo de interfaz, aunque los caracteres que envíe la tarjeta igualmente podrán estar separados por 12 etu. Este principio también es cierto para el carácter ACK que envía la tarjeta después de que el dispositivo de interfaz haya emitido un carácter P3.

— El dispositivo de interfaz deberá tener en cuenta los caracteres NUL que pueda emitir la tarjeta.

— El dispositivo de interfaz deberá aceptar el modo complementario de ACK.

— El comando GET RESPONSE no se puede utilizar en el modo de encadenamiento para obtener un dato cuya longitud podría sobrepasar 255 bytes.

TCS_16 **T=1**

— NAD Byte: no se utiliza (la dirección NAD deberá configurarse a '00').

— S-block ABORT: no se utiliza.

— S-block VPP state error: no se utiliza.

— La longitud total de encadenamiento de un campo de datos no sobrepasará 255 bytes (de ello se asegurará el IFD).

— El IFD deberá indicar el dispositivo de tamaño del campo de información (IFSD) inmediatamente después de la respuesta ATR: el IFD deberá transmitir la petición de S-Block IFS después de la ATR y la tarjeta deberá enviar el S-Block IFS. El valor recomendado para el IFSD es 254 bytes.

— La tarjeta no pedirá un reajuste del IFS.

3.2.2 *ATR*

TCS_17 El dispositivo comprueba los bytes ATR, de acuerdo con la norma ISO/CEI 7816-3. No se verificarán los caracteres históricos ATR.

Ejemplo de biprotocolo básico ATR con arreglo a la norma ISO/CEI 7816-3

Character	Value	Remarks
TS	'3Bh'	Indicates direct convention.
T0	'85h'	TD1 present; 5 historical bytes are presents.
TD1	'80h'	TD2 present; T=0 to be used
TD2	'11h'	TA3 present; T=1 to be used
TA3	'XXh' (at least 'F0h')	Information Field Size Card (IFSC)
TH1 to TH5	'XXh'	Historical characters
TCK	'XXh'	Check Character (exclusive OR)

TCS_18 Después de la Answer To Reset (ATR), el archivo principal (MF) se selecciona de manera implícita y pasa a ser el directorio actual.

3.2.3 *PTS*

TCS_19 El protocolo por defecto es T=0. Para configurar el protocolo T=1, es preciso que el dispositivo envíe a la tarjeta una selección PTS (también denominada PPS).

TCS_20 Dado que tanto el protocolo T=0 como el T=1 son obligatorios para la tarjeta, la selección PTS básica de conmutación de protocolos es obligatoria para la tarjeta.

La selección PTS se puede utilizar, tal y como se indica en la norma ISO/CEI 7816-3, para cambiar a una velocidad en baudios más alta que la velocidad que propone por defecto la tarjeta en la respuesta ATR, en su caso [byte TA(1)].

Opcionalmente, la tarjeta puede funcionar a velocidad en baudios más altas.

TCS_21 Si no se admiten otras velocidades en baudios aparte de la que se ajusta por defecto (o si la velocidad en baudios seleccionada es inadmisible), la tarjeta deberá responder a la selección PTS en la forma correcta según la norma ISO/CEI 7816-3, es decir, omitiendo el byte PPS1.

A continuación se ofrecen varios ejemplos de PTS básica selección de protocolo:

Character	Value	Remarks
PPSS	'FFh'	The Initiate Character.
PPS0	'00h' or '01h'	PPS1 to PPS3 are not present; '00h' to select T0, '01h' to select T1.
PK	'XXh'	Check Character: 'XXh' = 'FFh' if PPS0 = '00h', 'XXh' = 'FEh' if PPS0 = '01h'.

3.3. **Normas de acceso**

TCS_22 Una norma de acceso especifica las condiciones de seguridad correspondientes para un modo de acceso, es decir, un comando. Si se cumplen estas condiciones de seguridad, se procesa el comando correspondiente.

TCS_23 Se utilizan las condiciones de seguridad siguientes para la tarjeta de tacógrafo:

Abreviación	Significado
ALW	La acción siempre es posible y se puede ejecutar sin restricciones. El comando y la respuesta APDU se envían en texto simple, es decir, sin mensajería segura.
NEV	La acción nunca es posible.
PLAIN-C	El comando APDU se envía en texto simple, es decir, sin mensajería segura.
PWD	La acción solo puede ejecutarse si el PIN de la tarjeta de taller se verifica correctamente, es decir, si se ha configurado el estado de seguridad interna de la tarjeta 'PIN_Verified'. El comando debe enviarse sin mensajería segura.
EXT-AUT-G1	La acción puede ejecutarse solo si se ha ejecutado correctamente el comando External Authenticate para la autenticación de generación 1 (véase también la parte A del apéndice 11).
SM-MAC-G1	El APDU (comando y respuesta) debe aplicarse con mensajería segura de generación 1 en modo exclusivamente de autenticación (véase la parte A del apéndice 11).
SM-C-MAC-G1	El comando APDU debe aplicarse con mensajería segura de generación 1 en modo exclusivamente de autenticación (véase la parte A del apéndice 11).
SM-R-ENC-G1	La respuesta APDU debe aplicarse con mensajería segura de generación 1 en modo de cifrado (véase la parte A del apéndice 11), es decir, no se devuelve ningún código de autenticación de mensajes.
SM-R-ENC-MAC-G1	La respuesta APDU debe aplicarse con mensajería segura de generación 1 en modo de cifrado y posteriormente autenticación (véase la parte A del apéndice 11).
SM-MAC-G2	El APDU (comando y respuesta) debe aplicarse con mensajería segura de generación 2 en modo exclusivamente de autenticación (véase la parte B del apéndice 11).
SM-C-MAC-G2	El comando APDU debe aplicarse con mensajería segura de generación 2 en modo exclusivamente de autenticación (véase la parte B del apéndice 11).
SM-R-ENC-MAC-G2	La respuesta APDU debe aplicarse con mensajería segura de generación 2 en modo de cifrado y posteriormente autenticación (véase la parte B del apéndice 11).

TCS_24 Estas condiciones de seguridad pueden enlazarse de los modos siguientes:

AND: deben cumplirse todas las condiciones de seguridad;

OR: debe cumplirse al menos una condición de seguridad.

Las normas de acceso para el sistema de archivos, es decir, los comandos SELECT, READ BINARY y UPDATE BINARY, se especifican en el apartado 4. Las normas de acceso para el resto de comandos se especifican en las tablas siguientes.

TCS_25 En la aplicación DF tacógrafo G1, se utilizan las siguientes normas de acceso:

Comando	Tarjeta del conductor	Tarjeta de centro de ensayo	Tarjeta de control	Tarjeta de la empresa
External Authenticate				
— Para autenticación de generación 1	ALW	ALW	ALW	ALW
— Para autenticación de generación 2	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	No aplicable	No aplicable	No aplicable	No aplicable
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	No aplicable	No aplicable
PSO: Hash	No aplicable	No aplicable	ALW	No aplicable
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	No aplicable	No aplicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	No aplicable	No aplicable	ALW	No aplicable
Verify	No aplicable	ALW	No aplicable	No aplicable

TCS_26 En la aplicación DF tacógrafo_G2, se utilizan las siguientes normas de acceso:

Comando	Tarjeta del conductor	Tarjeta de centro de ensayo	Tarjeta de control	Tarjeta de la empresa
External Authenticate				
— Para autenticación de generación 1	No aplicable	No aplicable	No aplicable	No aplicable
— Para autenticación de generación 2	ALW	PWD	ALW	ALW
Internal Authenticate	No aplicable	No aplicable	No aplicable	No aplicable

Comando	Tarjeta del conductor	Tarjeta de centro de ensayo	Tarjeta de control	Tarjeta de la empresa
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	No aplicable	ALW	ALW	No aplicable
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	No aplicable	No aplicable
PSO: Hash	No aplicable	No aplicable	ALW	No aplicable
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	No aplicable	No aplicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	No aplicable	No aplicable	ALW	No aplicable
Verify	No aplicable	ALW	No aplicable	No aplicable

TCS_27 En el MF, se utilizan las siguientes normas de acceso:

Comando	Tarjeta del conductor	Tarjeta de centro de ensayo	Tarjeta de control	Tarjeta de la empresa
External Authenticate				
— Para autenticación de generación 1	No aplicable	No aplicable	No aplicable	No aplicable
— Para autenticación de generación 2	ALW	PWD	ALW	ALW
Internal Authenticate	No aplicable	No aplicable	No aplicable	No aplicable
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	No aplicable	No aplicable	No aplicable	No aplicable

Comando	Tarjeta del conductor	Tarjeta de centro de ensayo	Tarjeta de control	Tarjeta de la empresa
PSO: Compute Digital Signature	No aplicable	No aplicable	No aplicable	No aplicable
PSO: Hash	No aplicable	No aplicable	No aplicable	No aplicable
PSO: Hash of File	No aplicable	No aplicable	No aplicable	No aplicable
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	No aplicable	ALW	No aplicable	No aplicable

TCS_28 Una tarjeta de tacógrafo puede o no aceptar un comando con un nivel de seguridad superior al especificado en las condiciones de seguridad. Es decir, si la condición de seguridad es ALW (o PLAIN-C), la tarjeta puede aceptar un comando con mensajería segura (modo de cifrado y/o autenticación). Si la condición de seguridad requiere mensajería segura con modo de autenticación, la tarjeta del tacógrafo puede aceptar un comando con mensajería segura de la misma generación en modo de autenticación y cifrado.

Nota: Las descripciones de los comandos ofrecen más información acerca de la compatibilidad de los comandos con distintos tipos de tarjetas de tacógrafo y diferentes DF.

3.4. **Visión general de los comandos y los códigos de error**

Los comandos y la organización de archivos se deducen de la norma ISO/CEI 7816-4 y se ajustan a ella.

En esta sección se describen los siguientes pares comando APDU-respuesta. Las variantes de comandos que admite una aplicación de generación 1 y 2 se especifican en las descripciones correspondientes de los comandos.

Comando	INS
SELECT	'A4h'
READ BINARY	'B0h', 'B1h'
UPDATE BINARY	'D6h', 'D7h'
GET CHALLENGE	'84h'
VERIFY	'20h'
GET RESPONSE	'C0h'
PERFORM SECURITY OPERATION	'2Ah'
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	

Comando	INS
INTERNAL AUTHENTICATE	'88h'
EXTERNAL AUTHENTICATE	'82h'
MANAGE SECURITY ENVIRONMENT	'22h'
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	'86h'

TCS_29 Las palabras de estado SW1 SW2 aparecen en todos los mensajes de respuesta e indican el estado de procesado del comando.

SW1	SW2	Significado
90	00	Procesamiento normal.
61	XX	Procesamiento normal. XX = número de bytes de respuesta disponibles.
62	81	Procedimiento de aviso. Una parte de los datos devueltos puede estar dañada
63	00	Ha fallado la autenticación (Advertencia)
63	CX	CHV (PIN) incorrecto. 'X' indica el contador de intentos restantes
64	00	Error de ejecución. No ha variado el estado de la memoria permanente. Error de integridad.
65	00	Error de ejecución. Ha variado el estado de la memoria permanente
65	81	Error de ejecución. Ha variado el estado de la memoria permanente. Fallo de memoria
66	88	Error de seguridad: suma de control criptográfica incorrecta (durante la mensajería segura) o bien certificado incorrecto (durante la verificación del certificado) o bien criptograma incorrecto (durante la autentificación externa) o bien firma incorrecta (durante la verificación de la firma)
67	00	Longitud incorrecta (Lc o Le incorrecta)
68	82	Mensajería segura no admitida
68	83	Último comando de la cadena esperado
69	00	Comando prohibido (no hay respuesta disponible en T=0)
69	82	Estado de seguridad no satisfecho.
69	83	Método de autentificación bloqueado.
69	85	Condiciones de uso no satisfechas.
69	86	Comando no autorizado (falta el EF actual).

SW1	SW2	Significado
69	87	Faltan objetos de datos de mensajería segura que se esperaban.
69	88	Objetos de datos de mensajería segura incorrectos.
6A	80	Parámetros incorrectos en el campo de datos
6A	82	Archivo no encontrado.
6A	86	Parámetros P1-P2 incorrectos.
6A	88	Datos referenciados no encontrados.
6B	00	Parámetros incorrectos (desviación fuera del EF).
6C	XX	Longitud incorrecta, SW2 indica la longitud exacta. No se devuelve un campo de datos.
6D	00	Código de instrucción no admitido o no válido.
6E	00	Clase no admitida.
6F	00	Otros errores de comprobación

TCS_30 Si se cumplen más de una condición de error en un comando APDU, la tarjeta puede devolver cualquiera de las palabras de estado adecuada.

3.5. **Descripción de los comandos**

En el presente apartado se describen los comandos obligatorios para las tarjetas de tacógrafo.

En el apéndice 11 (Mecanismos de seguridad comunes) hallará otros pormenores relevantes relacionados con las operaciones criptográficas que es preciso realizar para tacógrafos de generación 1 y generación 2.

Todos los comandos se describen con independencia del protocolo utilizado (T=0 o T=1). Los bytes APDU CLA, INS, P1, P2, Lc y Le siempre se indican. Si el byte Lc o Le no es necesario para el comando descrito, entonces la longitud, el valor y la descripción asociados están vacíos.

TCS_31 Si se solicitan los dos bytes de longitud (Lc y Le) y además el IFD está utilizando el protocolo T=0, es preciso dividir en dos partes el comando descrito: el IFD envía el comando del modo descrito con P3 = Lc + datos y seguidamente envía un comando GET RESPONSE (véase § 3.5.6) con P3=Le.

TCS_32 Si se solicitan los dos bytes de longitud y Le=0 (mensajería segura):

— en caso de utilizarse el protocolo T=1, la tarjeta deberá responder a Le=0 enviando todos los datos de salida disponibles;

— en caso de utilizarse el protocolo T=0, el IFD deberá enviar el primer comando con P3 = Lc + datos, la tarjeta deberá responder (a este Le=0 implícito) con los bytes de estado '**61La**', donde La es el número de bytes de respuesta disponibles. A continuación, el IFD deberá generar un comando GET RESPONSE con P3 = La para leer los datos.

TCS_33 Una tarjeta de tacógrafo podría admitir campos de longitud ampliada conforme a ISO/CEI 7816-4 como función opcional. Una tarjeta de tacógrafo que admita campos de longitud ampliada deberá:

— indicar la compatibilidad con los campos de longitud ampliada en la ATR;

— proporcionar los tamaños de memoria temporal admitidos por medio de la información de longitud ampliada en el EF ATR/INFO, véase TCS_146;

— indicar si admite campos de longitud ampliada para T = 1 y/o T = 0 en la longitud ampliada de EF, véase TCS_147;

— admitir campos de longitud ampliada para la aplicación de tacógrafo de generación 1 y 2.

Notas:

Las especificaciones de todos los comandos son para campos de longitud corta. El uso de APDU de longitud ampliada está claro en ISO/CEI 7816-4.

Por lo general, se especifican los comandos para el modo director, es decir, sin mensajería segura, ya que la capa de mensajería segura se especifica en el apéndice 11. Se deduce claramente de las normas de acceso de un comando si este debe admitir mensajería segura o no y si el comando debe admitir mensajería segura de generación 1 y/o generación 2. Algunas variantes de comandos se describen con mensajería segura para ilustrar el uso de la mensajería segura.

TCS_34 La VU deberá ejecutar todo el protocolo de autenticación mutua de generación 2 VU-tarjeta durante una sesión, incluida la verificación de certificados (en caso necesario) ya sea en el DF tacógrafo, en el DF tacógrafo_G2 o en el MF.

3.5.1 *SELECT*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando SELECT se utiliza:

— para seleccionar un DF de la aplicación (es preciso utilizar la selección por nombre),

— para seleccionar un archivo elemental que corresponda al ID de archivo enviado.

3.5.1.1 Selección por nombre (AID)

Este comando permite seleccionar un DF de la aplicación en la tarjeta.

TCS_35 Este comando puede ejecutarse desde cualquier punto de la estructura de archivos (después de la respuesta ATR o en cualquier momento).

TCS_36 Al seleccionar una aplicación se reinicia el entorno de seguridad actual. Tras realizar la selección de la aplicación, ya no se selecciona ninguna clave pública actual. También se pierde la condición de acceso EXT-AUT-G1. Si el comando se ejecutó sin mensajería segura, las claves de la sesión de mensajería segura anterior dejan de estar disponibles.

TCS_37 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Selección por nombre (AID)
P2	1	'0Ch'	No se espera respuesta
Lc	1	'NNh'	Número de bytes enviados a la tarjeta (longitud del AID): '06h' para la aplicación de tacógrafo
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' para la aplicación de tacógrafo de generación 1 AID: 'FF 53 4D 52 44 54' para la aplicación de tacógrafo de generación 2

No se precisa respuesta para el comando SELECT (Le ausente en T=1, o no se pide respuesta en T=0).

TCS_38 **Mensaje de respuesta (no se pide respuesta)**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se encuentra la aplicación que corresponde al AID, se contesta con el estado de procesado '**6A82**'.

— En T=1, si está presente el byte Le, se contesta con el estado '**6700**'.

— En T=0, si se pide una respuesta después del comando SELECT, se contesta con el estado '**6900**'.

— Si se considera que la aplicación seleccionada está dañada (se detecta un error de integridad dentro de los atributos del archivo), se contesta con el estado de procesado '**6400**' o '**6581**'.

3.5.1.2 Selección de un archivo elemental utilizando su identificador de archivo

TCS_39 **Mensaje de comando**

TCS_40 Una tarjeta de tacógrafo deberá admitir mensajería segura de generación 2 tal como se especifica en la parte B del apéndice 11 para esta variante de comando.

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Selección de un EF bajo el DF actual
P2	1	'0Ch'	No se espera respuesta
Lc	1	'02h'	Número de bytes enviados a la tarjeta
#6-#7	2	'XXXXh'	Identificador de archivo

No se precisa respuesta para el comando SELECT (Le ausente en T=1, o no se pide respuesta en T=0).

TCS_41 **Mensaje de respuesta (no se pide respuesta)**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se encuentra el archivo que corresponde al identificador, se contesta con el estado de procesado '**6A82**'.

— En T=1, si está presente el byte Le, se contesta con el estado '**6700**'.

— En T=0, si se pide una respuesta después del comando SELECT, se contesta con el estado '**6900**'.

— Si se considera que el archivo seleccionado está dañado (se detecta un error de integridad dentro de los atributos del archivo), se contesta con el estado de procesado '**6400**' o '**6581**'.

3.5.2 *READ BINARY*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando READ BINARY sirve para leer datos de un archivo transparente.

La respuesta de la tarjeta consiste en devolver los datos leídos, opcionalmente encapsulados en una estructura de mensajería segura.

3.5.2.1 Comando con desviación en P1-P2

Este comando permite al IFD leer datos del EF actualmente seleccionado, sin mensajería segura.

Nota: Este comando sin mensajería segura solo puede utilizarse para leer un archivo que admita la condición de seguridad ALW para el modo de acceso de lectura.

TCS_42 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte más significativo
P2	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte menos significativo
Le	1	'XXh'	Longitud de los datos esperada. Número de bytes que se han de leer.

Nota: el bit 8 de P1 debe ponerse a 0.

TCS_43 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#X	X	'XX..XXh'	Datos leídos
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se selecciona un EF, se contesta con el estado de procesado '**6986**'.

— Si no se cumplen las condiciones de seguridad del archivo seleccionado, se interrumpe el comando con '**6982**'.

— Si la desviación no es compatible con el tamaño del EF (desviación > tamaño del EF), se contesta con el estado de procesado '**6B00**'.

— Si el tamaño de los datos que se han de leer no es compatible con el tamaño del EF (desviación + Le > tamaño del EF), se contesta con el estado de procesado '**6700**' o '**6Cxx**' donde 'xx' indica la longitud exacta.

— Si se detecta un error de integridad dentro de los atributos del archivo, la tarjeta considerará el archivo dañado e irrecuperable, se contesta con el estado de procesado '**6400**' o '**6581**'.

— Si se detecta un error de integridad dentro de los datos almacenados, la tarjeta devuelve los datos solicitados y contesta con el estado de procesado '**6281**'.

3.5.2.1.1 Comando con mensajería segura (ejemplos)

Este comando permite al IFD leer datos del EF actualmente seleccionado, con mensajería segura, a fin de verificar la integridad de los datos recibidos y proteger la confidencialidad de los datos si se aplica la condición de seguridad SM-R-ENC-MAC-G1 (generación 1) o SM-R-ENC-MAC-G2 (generación 2).

TCS_44 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'0Ch'	Se pide mensajería segura
INS	1	'B0h'	Read Binary
P1	1	'XXh'	P1 (desviación en bytes desde el comienzo del archivo): byte más significativo
P2	1	'XXh'	P2 (desviación en bytes desde el comienzo del archivo): byte menos significativo
Lc	1	'XXh'	Longitud de los datos de entrada para mensajería segura
#6	1	'97h'	T_{LE}: Etiqueta para especificación de la longitud esperada.
#7	1	'01h'	L_{LE}: Longitud de la longitud esperada
#8	1	'NNh'	Especificación de la longitud esperada (Le original): Número de bytes que se han de leer
#9	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#10	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '04h' para mensajería segura de generación 1 (véase la parte A del apéndice 11) '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#11-#(10+L)	L	'XX..XXh'	Cryptographic checksum (suma de control criptográfica),
Le	1	'00h'	Según se especifica en la norma ISO/CEI 7816-4

TCS_45 **Mensaje de respuesta si no se requiere SM-R-ENC-MAC-G1 (generación 1) / SM-R-ENC-MAC-G2 (generación 2) y si el formato de entrada de mensajería segura es correcto:**

Byte	Longitud	Valor	Descripción
#1	1	'99h'	Etiqueta para el estado de procesado (SW1-SW2) — opcional para mensajería segura de generación 1
#2	1	'02h'	Longitud del estado de procesado
#3 — #4	2	'XX XXh'	Estado de procesado de la respuesta APDU sin proteger
#5	1	'81h'	T_{PV}: Etiqueta para datos del valor plano
#6	L	'NNh' o '81 NNh'	L_{PV}: longitud de los datos devueltos (=Le original). L es 2 bytes si L_{PV} > 127 bytes

Byte	Longitud	Valor	Descripción
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Valor de datos planos
#(6+L+NN)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(7+L+NN)	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '04h' para mensajería segura de generación 1 (véase la parte A del apéndice 11) '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Suma de control criptográfica
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

TCS_46 **Mensaje de respuesta si se requiere SM-R-ENC-MAC-G1 (generación 1) / SM-R-ENC-MAC-G2 (generación 2) y si el formato de entrada de mensajería segura es correcto:**

Byte	Longitud	Valor	Descripción
#1	1	'87h'	$T_{PI\ CG}$: Etiqueta para datos cifrados (criptograma)
#2	L	'MMh' o '81 MMh'	$L_{PI\ CG}$: longitud de los datos cifrados que se devuelven (distinta de la Le original del comando, debido al relleno). L es 2 bytes si $L_{PI\ CG}$ > 127 bytes
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Datos cifrados: Indicador de relleno y criptograma
#(2+L+MM)	1	'99h'	Etiqueta para el estado de procesado (SW1-SW2) — opcional para mensajería segura de generación 1
#(3+L+MM)	1	'02h'	Longitud del estado de procesado
#(4+L+MM) — #(5+L+MM)	2	'XX XXh'	Estado de procesado de la respuesta APDU sin proteger
#(6+L+MM)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(7+L+MM)	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '04h' para mensajería segura de generación 1 (véase la parte A del apéndice 11) '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Suma de control criptográfica
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

El comando READ BINARY puede devolver estados de procesado normales enumerados en TCS_43 bajo la etiqueta '99h' tal como se describe en TCS_59 utilizando la estructura de respuesta de mensajería segura.

Asimismo, es posible que se produzcan algunos errores específicamente relacionados con la mensajería segura. En tal caso, el estado de procesado se devuelve tal cual, sin la intervención de una estructura de mensajería segura.

TCS_47 **Mensaje de respuesta si el formato de entrada de mensajería segura es incorrecto**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si no hay una clave disponible para la sesión actual, se devuelve el estado de procesado '**6A88**'. Esto ocurre si la clave de la sesión no se ha generado todavía o si ha expirado la validez de dicha clave (en tal caso, el IFD debe ejecutar de nuevo un proceso de autentificación mutua para establecer una nueva clave de sesión).

— Si en el formato de mensajería segura faltan algunos de los objetos de datos que se esperaban (anteriormente especificados), se devuelve el estado de procesado '**6987**': este error se produce si falta una etiqueta esperada o si el cuerpo del comando no está bien construido.

— Si algunos de los objetos de datos son incorrectos, se contesta con el estado de procesado '**6988**': este error se produce si están presentes todas las etiquetas necesarias pero algunas longitudes no coinciden con las esperadas.

— Si falla la verificación de la suma de control criptográfica, se contesta con el estado de procesado '**6688**'.

3.5.2.2 Comando con identificador EF (archivo elemental) corto

Esta variante de comando permite al IFD seleccionar un EF por medio de un identificador EF corto y leer los datos de este EF.

TCS_48 Una tarjeta de tacógrafo deberá admitir esta variante de comando para todos los archivos elementales que lleven especificado un identificador EF corto. Estos identificadores EF cortos se especifican en el apartado 4.

TCS_49 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	El bit 8 se pone en 1 Los bits 7 y 6 se ponen en 00 Los bits 5 a 1 codifican el identificador EF corto del EF correspondiente
P2	1	'XXh'	Codifica una desviación desde 0 hasta 255 bytes en el EF referenciado por P1
Le	1	'XXh'	Longitud de los datos esperada. Número de bytes que se han de leer.

Nota: Los identificadores EF cortos utilizados para la aplicación de tacógrafo de generación 2 se especifican en el apartado 4.

Si P1 codifica un identificador EF corte y el comando es correcto, el EF identificado pasa a ser el EF seleccionado actualmente (EF actual).

TCS_50 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#L	L	'XX..XXh'	Datos leídos
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se encuentra el archivo que corresponde al identificador EF corto, se contesta con el estado de procesado '**6A82**'.

— Si no se satisfacen las condiciones de seguridad del archivo seleccionado, se interrumpe el comando con '**6982**'.

— Si la desviación no es compatible con el tamaño del EF (desviación > tamaño del EF), se contesta con el estado de procesado '**6B00**'.

— Si el tamaño de los datos que se han de leer no es compatible con el tamaño del EF (desviación + Le > tamaño del EF), se contesta con el estado de procesado '**6700**' o '**6Cxx**' donde 'xx' indica la longitud exacta.

— Si se detecta un error de integridad dentro de los atributos del archivo, la tarjeta considerará el archivo dañado e irrecuperable, se contesta con el estado de procesado '**6400**' o '**6581**'.

— Si se detecta un error de integridad dentro de los datos almacenados, la tarjeta devuelve los datos solicitados y contesta con el estado de procesado '**6281**'.

3.5.2.3 Comando con byte de instrucción impar

Esta variante de comando permite al IFD leer datos de un EF de 32 768 bytes o más.

TCS_51 Una tarjeta de tacógrafo que admita EF de 32 768 bytes o más deberá admitir esta variante de comando para estos EF. Una tarjeta de tacógrafo puede o no admitir esta variante de comando para otros EF a excepción del EF Sensor_Installation_Data; véase TCS_156 y TCS_160.

TCS_52 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	EF actual
P2	1	'00h'	
Lc	1	'NNh'	Lc longitud del objeto de datos de desviación.
#6-#(5+NN)	NN	'XX..XXh'	Objeto de datos de desviación: Etiqueta '54h' Longitud '01h' o '02h' Valor desviación
Le	1	'XXh'	Número de bytes que se han de leer.

El IFD deberá codificar la longitud del objeto de datos de desviación con un número mínimo posible de octetos, es decir, utilizando el byte de longitud '01h' el IFD deberá codificar una desviación comprendida entre 0 y 255 y, mediante el byte de longitud '02h', una desviación comprendida entre '256' y '65 535' bytes.

TCS_53 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#L	L	'XX..XXh'	Datos leídos encapsulados en un objeto de datos discrecional con etiqueta '53h'.
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se selecciona un EF, se contesta con el estado de procesado '**6986**'.

— Si no se satisfacen las condiciones de seguridad del archivo seleccionado, se interrumpe el comando con '**6982**'.

— Si la desviación no es compatible con el tamaño del EF (desviación > tamaño del EF), se contesta con el estado de procesado '**6B00**'.

— Si el tamaño de los datos que se han de leer no es compatible con el tamaño del EF (desviación + Le > tamaño del EF), se contesta con el estado de procesado '**6700**' o '**6Cxx**' donde 'xx' indica la longitud exacta.

— Si se detecta un error de integridad dentro de los atributos del archivo, la tarjeta considerará el archivo dañado e irrecuperable, se contesta con el estado de procesado '**6400**' o '**6581**'.

— Si se detecta un error de integridad dentro de los datos almacenados, la tarjeta devuelve los datos solicitados y contesta con el estado de procesado '**6281**'.

3.5.2.3.1 Comando con mensajería segura (ejemplo)

El siguiente ejemplo ilustra el uso de la mensajería segura si se aplica la condición de seguridad SM-MAC-G2.

TCS_54 Mensaje de comando

Byte	Longitud	Valor	Descripción
CLA	1	'0Ch'	Se pide mensajería segura
INS	1	'B1h'	Read Binary
P1	1	'00h'	EF actual
P2	1	'00h'	
Lc	1	'XXh'	Longitud del campo de datos seguro
#6	1	'B3h'	Etiqueta para datos del valor plano codificados en BER-TLV
#7	1	'NNh'	L_{PV}: longitud de los datos transmitidos
#(8)-#(7+NN)	NN	'XX..XXh'	Datos planos codificados en BER-TLV, es decir, el objeto de datos de desviación con etiqueta '54'
#(8+NN)	1	'97h'	T_{LE}: Etiqueta para especificación de la longitud esperada.
#(9+NN)	1	'01h'	L_{LE}: Longitud de la longitud esperada
#(10+NN)	1	'XXh'	Especificación de la longitud esperada (Le original): Número de bytes que se han de leer
#(11+NN)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(12+NN)	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Suma de control criptográfica
Le	1	'00h'	Según se especifica en la norma ISO/CEI 7816-4

TCS_55 Mensaje de respuesta si el comando es correcto

Byte	Longitud	Valor	Descripción
#1	1	'B3h'	Datos planos codificados en BER-TLV
#2	L	'NNh' o '81 NNh'	L_{PV}: longitud de los datos devueltos (=Le original). L es 2 bytes si L_{PV} > 127 bytes
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Valor de datos planos codificados en BER-TLV, es decir, los datos leídos encapsulados en un objeto de datos discrecional con etiqueta '53h'.
#(2+L+NN)	1	'99h'	Estado de procesado de la respuesta APDU sin proteger
#(3+L+NN)	1	'02h'	Longitud del estado de procesado
#(4+L+NN) — #(5+L+NN)	2	'XX XXh'	Estado de procesado de la respuesta APDU sin proteger
#(6+L+NN)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(7+L+NN)	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Suma de control criptográfica
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

3.5.3 *UPDATE BINARY*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El mensaje de comando UPDATE BINARY inicia la actualización (borrar + escribir) de los bits ya presentes en un EF binario, para sustituirlos por los bits dados en el comando APDU.

3.5.3.1 Comando con desviación en P1-P2

Este comando permite al IFD escribir datos en el EF actualmente seleccionado, sin que la tarjeta verifique la integridad de los datos recibidos.

Nota: Este comando sin mensajería segura solo puede utilizarse para leer un archivo que admita la condición de seguridad ALW para el modo de acceso de actualización.

TCS_56 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'D6h'	Update Binary

Byte	Longitud	Valor	Descripción
P1	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte más significativo
P2	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte menos significativo
Lc	1	'NNh'	Lc Longitud de los datos que se han de actualizar. Número de bytes que se han de escribir.
#6-#(5+NN)	NN	'XX..XXh'	Datos que se han de escribir

Nota: el bit 8 de P1 debe ponerse a 0.

TCS_57 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se selecciona un EF, se contesta con el estado de procesado '**6986**'.

— Si no se satisfacen las condiciones de seguridad del archivo seleccionado, se interrumpe el comando con '**6982**'.

— Si la desviación no es compatible con el tamaño del EF (desviación > tamaño del EF), se contesta con el estado de procesado '**6B00**'.

— Si el tamaño de los datos que se han de escribir no es compatible con el tamaño del EF (desviación + Lc > tamaño del EF), se contesta con el estado de procesado '**6700**'.

— Si se detecta un error de integridad dentro de los atributos del archivo, la tarjeta considerará el archivo dañado e irrecuperable, se contesta con el estado de procesado '**6400**' o '**6500**'.

— Si falla la escritura, se contesta con el estado de procesado '**6581**'.

3.5.3.1.1 Comando con mensajería segura (ejemplos)

Este comando permite al IFD escribir datos en el EF actualmente seleccionado, de modo que la tarjeta verifica la integridad de los datos recibidos. Dado que no se precisa confidencialidad, los datos no están cifrados.

TCS_58 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'0Ch'	Se pide mensajería segura
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte más significativo
P2	1	'XXh'	Desviación en bytes desde el comienzo del archivo: byte menos significativo
Lc	1	'XXh'	Longitud del campo de datos seguro

Byte	Longitud	Valor	Descripción
#6	1	'81h'	T_{PV}: Etiqueta para datos del valor plano
#7	L	'NNh' o '81 NNh'	L_{PV}: longitud de los datos transmitidos. L es 2 bytes si L_{PV} > 127 bytes.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Valor de datos planos (datos que se han de escribir)
#(7+L+NN)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(8+L+NN)	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '04h' para mensajería segura de generación 1 (véase la parte A del apéndice 11) '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Suma de control criptográfica
Le	1	'00h'	Según se especifica en la norma ISO/CEI 7816-4

TCS_59 **Mensaje de respuesta si el formato de entrada de mensajería segura es correcto**

Byte	Longitud	Valor	Descripción
#1	1	'99h'	T_{SW}: Etiqueta para palabras de estado (con la protección de CC)
#2	1	'02h'	L_{SW}: longitud de las palabras de estado devueltas
#3-#4	2	'XXXXh'	Estado de procesado de la respuesta APDU sin proteger
#5	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#6	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '04h' para mensajería segura de generación 1 (véase la parte A del apéndice 11) '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#7-#(6+L)	L	'XX..XXh'	Suma de control criptográfica
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

Los estados de procesado «normales», descritos para el comando UPDATE BINARY sin mensajería segura (véase §3.5.3.1), se pueden devolver utilizando las estructuras de mensaje de respuesta descritas anteriormente.

Asimismo, es posible que se produzcan algunos errores específicamente relacionados con la mensajería segura. En tal caso, el estado de procesado se devuelve tal cual, sin la intervención de una estructura de mensajería segura.

TCS_60 **Mensaje de respuesta si se produce un error de mensajería segura**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si no hay una clave disponible para la sesión actual, se devuelve el estado de procesado '**6A88**'.

— Si en el formato de mensajería segura faltan algunos de los objetos de datos que se esperaban (anteriormente especificados), se devuelve el estado de procesado '**6987**': este error se produce si falta una etiqueta esperada o si el cuerpo del comando no está bien construido.

— Si algunos de los objetos de datos son incorrectos, se contesta con el estado de procesado '6988': este error se produce si están presentes todas las etiquetas necesarias pero algunas longitudes no coinciden con las esperadas.

— Si falla la verificación de la suma de control criptográfica, se contesta con el estado de procesado '**6688**'.

3.5.3.2 Comando con identificador EF corto

Esta variante de comando permite al IFD seleccionar un EF por medio de un identificador EF corto y escribir los datos de este EF.

TCS_61 Una tarjeta de tacógrafo deberá admitir esta variante de comando para todos los archivos elementales que lleven especificado un identificador EF corto. Estos identificadores EF cortos se especifican en el apartado 4.

TCS_62 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	El bit 8 se pone en 1 Los bits 7 y 6 se ponen en 00 Los bits 5 a 1 codifican el identificador EF corto del EF correspondiente
P2	1	'XXh'	Codifica una desviación desde 0 hasta 255 bytes en el EF referenciado por P1
Lc	1	'NNh'	Lc Longitud de los datos que se han de actualizar. Número de bytes que se han de escribir.
#6-#(5+NN)	NN	'XX..XXh'	Datos que se han de escribir

TCS_63 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

Nota: Los identificadores EF cortos utilizados para la aplicación de tacógrafo de generación 2 se especifican en el apartado 4.

Si P1 codifica un identificador EF corte y el comando es correcto, el EF identificado pasa a ser el EF seleccionado actualmente (EF actual).

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se encuentra el archivo que corresponde al identificador EF corto, se contesta con el estado de procesado '**6A82**'.

— Si no se satisfacen las condiciones de seguridad del archivo seleccionado, se interrumpe el comando con '**6982**'.

— Si la desviación no es compatible con el tamaño del EF (desviación > tamaño del EF), se contesta con el estado de procesado '**6B00**'.

— Si el tamaño de los datos que se han de escribir no es compatible con el tamaño del EF (desviación + Lc > tamaño del EF), se contesta con el estado de procesado '**6700**'.

— Si se detecta un error de integridad dentro de los atributos del archivo, la tarjeta considerará el archivo dañado e irrecuperable, se contesta con el estado de procesado '**6400**' o '**6581**'.

— Si falla la escritura, se contesta con el estado de procesado '**6581**'.

3.5.3.3 Comando con byte de instrucción impar

Esta variante de comando permite al IFD escribir datos de un EF de 32 768 bytes o más.

TCS_64 Una tarjeta de tacógrafo que admita EF de 32 768 bytes o más deberá admitir esta variante de comando para estos EF. Una tarjeta de tacógrafo puede o no admitir esta variante de comando para otros EF.

TCS_65 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	EF actual
P2	1	'00h'	
Lc	1	'NNh'	Lc Longitud de datos en el campo de datos del comando
#6-#(5+NN)	NN	'XX..XXh'	Objeto de datos de desviación con etiqueta '54h' || Objeto de datos discrecional con etiqueta '53h' que encapsula los datos que han de escribirse

El IFD deberá codificar la longitud del objeto de datos de desviación y el objeto de datos discrecional con un número mínimo posible de octetos, es decir, utilizando el byte de longitud '01h' el IFD deberá codificar una desviación/longitud comprendida entre 0 y 255 y, mediante el byte de longitud '02h', una desviación/longitud comprendida entre '256' y '65 535' bytes.

TCS_66 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se selecciona un EF, se contesta con el estado de procesado '**6986**'.

— Si no se satisfacen las condiciones de seguridad del archivo seleccionado, se interrumpe el comando con '**6982**'.

— Si la desviación no es compatible con el tamaño del EF (desviación > tamaño del EF), se contesta con el estado de procesado '**6B00**'.

— Si el tamaño de los datos que se han de escribir no es compatible con el tamaño del EF (desviación + Lc > tamaño del EF), se contesta con el estado de procesado '**6700**'.

— Si se detecta un error de integridad dentro de los atributos del archivo, la tarjeta considerará el archivo dañado e irrecuperable, se contesta con el estado de procesado '**6400**' o '**6500**'.

— Si falla la escritura, se contesta con el estado de procesado '**6581**'.

3.5.3.3.1 Comando con mensajería segura (ejemplo)

El siguiente ejemplo ilustra el uso de la mensajería segura si se aplica la condición de seguridad SM-MAC-G2.

TCS_67 Mensaje de comando

Byte	Longitud	Valor	Descripción
CLA	1	'0Ch'	Se pide mensajería segura
INS	1	'D7h'	Update Binary
P1	1	'00h'	EF actual
P2	1	'00h'	
Lc	1	'XXh'	Longitud del campo de datos seguro
#6	1	'B3h'	Etiqueta para datos del valor plano codificados en BER-TLV
#7	L	'NNh' o '81 NNh'	L_{PV}: longitud de los datos transmitidos. L es 2 bytes si L_{PV} > 127 bytes.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Datos planos codificados en BER-TLV, es decir, el objeto de datos de desviación con etiqueta '54h' || Objeto de datos discrecional con etiqueta '53h' que encapsula los datos que han de escribirse
#(7+L+NN)	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica
#(8+L+NN)	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Suma de control criptográfica
Le	1	'00h'	Según se especifica en la norma ISO/CEI 7816-4

TCS_68 Mensaje de respuesta si el comando es correcto

Byte	Longitud	Valor	Descripción
#1	1	'99h'	T_{SW}: Etiqueta para palabras de estado (con la protección de CC)
#2	1	'02h'	L_{SW}: longitud de las palabras de estado devueltas
#3-#4	2	'XXXXh'	Estado de procesado de la respuesta APDU sin proteger
#5	1	'8Eh'	T_{CC}: Etiqueta para suma de control criptográfica

Byte	Longitud	Valor	Descripción
#6	1	'XXh'	L_{CC}: Longitud de la siguiente suma de control criptográfica '08h', '0Ch' o '10h' dependiendo de la longitud de la clave AES para mensajería segura de generación 2 (véase la parte B del apéndice 11)
#7-#(6+L)	L	'XX..XXh'	Suma de control criptográfica
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

3.5.4 *GET CHALLENGE*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando GET CHALLENGE pide a la tarjeta que envíe una interrogación para usarla en un procedimiento relacionado con la seguridad que incluya el envío de un criptograma o de unos datos cifrados a la tarjeta.

TCS_69 La interrogación que envía la tarjeta tan solo es válida para el siguiente comando que utilice una interrogación y se envíe a la tarjeta.

TCS_70 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Longitud de la interrogación esperada)

TCS_71 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#8	8	'XX..XXh'	Interrogación
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si Le es distinto de '08h', el estado de procesado es '**6700**'.

— Si los parámetros P1-P2 son incorrectos, el estado de procesado es '**6A86**'.

3.5.5 *VERIFY*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

Solo la tarjeta de taller necesita admitir este comando.

Otros tipos de tarjetas de tacógrafo pueden o no incorporar este comando, pero para estas tarjetas no se personaliza ninguna información CHV de referencia. Por tanto, estas tarjetas no pueden realizar este comando correctamente. En cuanto al resto de tipos de tarjetas de tacógrafo que no sean tarjetas de taller, el comportamiento, es decir, el código de error devuelto, está fuera del alcance de esta especificación si se envía este comando.

El comando VERIFY inicia una comparación en la tarjeta, confrontando los datos CHV (PIN) enviados desde el comando con la información CHV de referencia almacenada en la tarjeta.

TCS_72 El IFD debe añadir bytes 'FFh' para rellenar por la derecha el PIN que introduzca el usuario y debe codificarse en ASCI, hasta llegar a una longitud de 8 bytes; véase también el tipo de datos WorkshopCardPIN en el apéndice 1.

TCS_73 Las aplicaciones de tacógrafo de generación 1 y 2 deberán utilizar la misma información CHV de referencia.

TCS_74 La tarjeta de tacógrafo deberá comprobar si el comando está codificado correctamente. Si el comando no está codificado correctamente, la tarjeta no comparará los valores CHV, no disminuirá el contador de intentos CHV restantes y no reiniciará el estado de seguridad «PIN_Verified», pero interrumpirá el comando. Un comando está codificado correctamente si los bytes CLA, INS, P1, P2, Lc tienen los valores especificados, Le está ausente y el campo de datos del comando tiene la longitud correcta.

TCS_75 Si el comando es correcto, el contador de intentos CHV restantes se reinicializa. El valor inicial del contador de intentos CHV restantes es 5. Si el comando es correcto, la tarjeta establecerá el estado de seguridad interna «PIN_Verified». La tarjeta restablecerá este estado de seguridad si se restablece la tarjeta o si el código CHV transmitido en el comando no coincide con la información CHV de referencia almacenada.

Nota: utilizar la misma información CHV de referencia y un estado de seguridad global evita que un empleado del taller tenga que volver a introducir el PIN tras seleccionar otro DF de la aplicación de tacógrafo.

TCS_76 En la tarjeta queda registrada cada comparación incorrecta, es decir, el contador de intentos CHV restantes disminuye en uno, a fin de limitar el número de intentos que quedan para utilizar la información CHV de referencia.

TCS_77 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (la CHV verificada se conoce implícitamente)
Lc	1	'08h'	Longitud del código CHV transmitido
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no se encuentra la referencia CHV, se contesta con el estado de procesado '**6A88**'.

— Si la información CHV está bloqueada (el contador de intentos restantes de la CHV es cero), se contesta con el estado de procesado '**6983**'. Una vez en ese estado, ya no se puede volver a presentar la información CHV.

— Si la comparación no tiene éxito, se resta una unidad a la lectura del contador de intentos restantes y se devuelve el estado '**63CX**' (X > 0 y X es igual al contador de intentos CHV restantes.

— Si se considera que la información CHV de referencia está dañada, se contesta con el estado de procesado '**6400**' o '**6581**'.

— Si Lc es distinto de '08h', el estado de procesado es '**6700**'.

3.5.6 *GET RESPONSE*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4.

Este comando (exclusivamente necesario y disponible en el protocolo T=0) sirve para transmitir datos preparados de la tarjeta al dispositivo de interfaz (cuando el comando incluye las longitudes Lc y Le).

El comando GET RESPONSE tiene que enviarse inmediatamente después del comando que prepara los datos. De lo contrario, los datos se pierden. Una vez ejecutado el comando GET RESPONSE (salvo si se produce el error '**61xx**' o '**6Cxx**', véase más abajo), los datos preparados previamente dejan de estar disponibles.

TCS_79 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Número de bytes esperados

TCS_80 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#X	X	'XX..XXh'	Datos
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si la tarjeta no ha preparado ningún dato, se contesta con el estado de procesado '**6900**' o '**6F00**'.

— Si la longitud Le sobrepasa el número de bytes disponibles o es igual a cero, se contesta con el estado de procesado '**6Cxx**', donde xx es el número exacto de bytes disponibles. En ese caso, los datos preparados siguen estando disponibles para un comando GET RESPONSE posterior.

— Si la longitud Le es distinta de cero y menor que el número de bytes disponibles, la tarjeta normalmente envía los datos necesarios y se contesta con el estado de procesado '**61xx**', donde 'xx' indica el número de bytes extra todavía disponibles para un comando GET RESPONSE posterior.

— Si el comando no se admite (protocolo T=1), la tarjeta contesta con el estado '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8, pero tiene un uso restringido en comparación con el comando que se define en dicha norma.

El comando VERIFY CERTIFICATE lo utiliza la tarjeta para obtener una clave pública del exterior y para comprobar su validez.

3.5.7.1 Comando de generación 1 — Par de respuestas

TCS_81 Esta variante de comando es compatible únicamente con una aplicación de tacógrafo de generación 1.

TCS_82 Cuando un comando VERIFY CERTIFICATE se ejecuta correctamente, la clave pública queda almacenada para su uso posterior en el entorno de seguridad. Esta clave debe crearla de forma explícita el comando MSE utilizando su identificador de clave (véase § 3.5.11) para uso en comandos relacionados con la seguridad (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE o VERIFY CERTIFICATE).

TCS_83 En cualquier caso, el comando VERIFY CERTIFICATE utiliza la clave pública previamente seleccionada por el comando MSE para abrir el certificado. Esta clave pública debe ser la de un Estado miembro o de Europa.

TCS_84 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'00h'	P1
P2	1	'AEh'	P2: datos sin codificación BER-TLV (concatenación de elementos de datos)
Lc	1	'C2h'	Lc: Longitud del certificado, 206 Bytes
#6-#199	194	'XX..XXh'	Certificado: concatenación de elementos de datos (como se describe en el apéndice 11)

TCS_85 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si la verificación del certificado falla, se contesta con el estado de procesado '**6688**'. El proceso de verificación y apertura del certificado se describe en el apéndice 11 para G1 y G2.

— Si no hay una clave pública presente en el entorno de seguridad, se devuelve '**6A88**'.

— Si se considera que la clave pública seleccionada (utilizada para desenvolver el certificado) está dañada, se contesta con el estado de procesado '**6400**' o '**6581**'.

— Generación 1 únicamente: Si la clave pública seleccionada (utilizada para desenvolver el certificado) tiene un CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) diferente de '00' (es decir, no es el de un Estado miembro o el de Europa), se contesta con el estado de procesado '**6985**'.

3.5.7.2 Comando de generación 2 — Par de respuestas

Dependiendo del tamaño de la curva, los certificados ECC pueden ser tan largos que no es posible transmitirlos en un solo APDU. En este caso, debe aplicarse el encadenamiento de comandos según ISO/CEI 7816-4 y el certificado debe transmitirse en dos PSO consecutivos: APDU de Verify Certificate.

La estructura del certificado y los parámetros de dominio se definen en el apéndice 11.

TCS_86 El comando puede ejecutarse en el MF, DF tacógrafo y DF tacógrafo_G2; véase también TCS_33.

TCS_87 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'X0h'	Byte CLA que indica el encadenamiento de comandos: '00h' el único comando o el último de la cadena '10h' no es el último comando de una cadena
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'00h'	
P2	1	'BEh'	Verificar certificado autodescriptivo
Lc	1	'XXh'	Longitud del campo de datos del comando, véase TCS_88TCS_88 y TCS_89TCS_89.
#6-#5+L	L	'XX..XXh'	Datos codificados en DER-TLV: Objeto de datos del cuerpo del certificado ECC como primer objeto de datos concatenado con el objeto de datos de la firma del certificado ECC como segundo objeto de datos o para de esta concatenación. La etiqueta '7F21' y la correspondiente longitud no deberán transmitirse. El orden de estos objetos de datos es fijo.

TCS_88 Para APDU de longitud corta, se aplican las siguientes disposiciones: El IFD deberá utilizar el número mínimo de APDU necesario para transmitir los datos útiles del comando y transmitir el máximo número de bytes en el primer comando APDU de acuerdo con el valor del tamaño del campo de información para la tarjeta; véase TCS_14TCS_14. Si el IFD se comporta de forma diferente, el comportamiento de la tarjeta está fuera del alcance.

TCS_89 Para APDU de longitud ampliada, se aplican las siguientes disposiciones: si el certificado no encaja en un solo APDU, la tarjeta deberá admitir el encadenamiento de comandos. El IFD deberá utilizar el número mínimo de APDU necesario para transmitir los datos útiles del comando y transmitir el máximo número de bytes en el primer comando APDU. Si el IFD se comporta de forma diferente, el comportamiento de la tarjeta está fuera del alcance.

Nota: Según el apéndice 11, la tarjeta almacena el certificado o el contenido relevante del certificado y actualiza su currentAuthenticatedTime.

La estructura del mensaje de respuesta y las palabras de estado son las que se definen en TCS_85TCS_85.

TCS_90 Además de los códigos de error enumerados en TCS_85TCS_85, la tarjeta puede devolver los siguientes códigos de error:

— Si la clave pública seleccionada (utilizada para desenvolver el certificado) tiene un CHA.LSB (CertificateHolderAuthorisation.equipmentType) que no es apropiado para la verificación de certificados según el apéndice 11, se contesta con el estado de procesado '**6985**'.

— Si el currentAuthenticatedTime de la tarjeta es posterior a la fecha de caducidad del certificado, se contesta con el estado de procesado '**6985**'.

— Si se espera el último comando de la cadena, la tarjeta contesta con el estado '**6883**'.

— Si se envían parámetros incorrectos en el campo de datos del comando, la tarjeta contesta con el estado '**6A80**' (utilizado también en caso de que los objetos de datos no se envíen en el orden especificado).

3.5.8 *INTERNAL AUTHENTICATE*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4.

TCS_91 Todas las tarjetas de tacógrafo deberán admitir este comando en el DF tacógrafo de generación 1. El comando puede o no estar accesible en el MF y/o el DF tacógrafo_G2. Si es así, el comando deberá terminar con un código de error apropiado ya que la clave privada de la tarjeta (Card.SK) para el protocolo de autenticación de generación 1 solo es accesible en el DF_tacógrafo de generación 1.

Por medio del comando INTERNAL AUTHENTICATE, el IFD puede autentificar la tarjeta. El proceso de autenticación se describe en el apéndice 11. Incluye las declaraciones siguientes:

TCS_92 El comando INTERNAL AUTHENTICATE utiliza la clave privada de la tarjeta (seleccionada implícitamente) para firmar datos de autentificación, incluidos K1 (el primer elemento para acordar la clave de la sesión) y RND1, y utiliza la clave pública actualmente seleccionada (a través del último comando MSE) para cifrar la firma y formar el testigo de autentificación (hallará información más detallada al respecto en el apéndice 11).

TCS_93 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Longitud de los datos enviados a la tarjeta
#6 — #13	8	'XX..XXh'	Interrogación empleada para autentificar la tarjeta
#14 -#21	8	'XX..XXh'	VU.CHR (véase el apéndice 11)
Le	1	'80h'	Longitud de los datos que se esperan de la tarjeta

TCS_94 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#128	128	'XX..XXh'	Testigo de autentificación de la tarjeta (véase el apéndice 11)
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si no hay una clave pública presente en el entorno de seguridad, se contesta con el estado de procesado '**6A88**'.

— Si no hay una clave privada presente en el entorno de seguridad, se contesta con el estado de procesado '**6A88**'.

— Si VU.CHR no coincide con el identificador actual de clave pública, se contesta con el estado de procesado '**6A88**'.

— Si se considera que la clave privada seleccionada está dañada, se contesta con el estado de procesado '**6400**' o '**6581**'.

TCS_95 Si el comando INTERNAL AUTHENTICATE se ejecuta correctamente, la clave de la sesión actual, si la hay, se borra y deja de estar disponible. Para disponer de una nueva clave de sesión, es preciso que se ejecute correctamente el comando EXTERNAL AUTHENTICATE para el mecanismo de autenticación de generación 1.

3.5.9 *EXTERNAL AUTHENTICATE*

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4.

Por medio del comando EXTERNAL AUTHENTICATE, la tarjeta puede autentificar el IFD. En el apéndice 11 se describe el proceso de autenticación del tacógrafo G1 y G2 (autenticación de la VU).

TCS_96 La variante del comando para el mecanismo de autenticación mutua de generación 1 es compatible únicamente con una aplicación de tacógrafo de generación 1.

TCS_97 La variante del comando para la autenticación mutua de la tarjeta de la VU de segunda generación puede ejecutarse en el MF, DF tacógrafo y DF tacógrafo_G2; véase también TCS_34TCS_34.

TCS_98 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Claves y algoritmos conocidos implícitamente
P2	1	'00h'	
Lc	1	'XXh'	Lc (Longitud de los datos enviados a la tarjeta)
#6-#(5+L)	L	'XX..XXh'	Autenticación de generación 1: Criptograma (véase la parte A del apéndice 11) Autenticación de generación 2: Firma generada por el IFD (véase la parte B del apéndice 11)

TCS_99 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si el CHA de la clave pública actualmente configurada no es la concatenación del AID de la aplicación de tacógrafo y de un tipo de equipo VU, se contesta con el estado de procesado '**6F00**'.

— Si el comando no va precedido inmediatamente de un comando GET CHALLENGE, se contesta con el estado de procesado '**6985**'.

La aplicación de tacógrafo de generación 1 puede devolver los siguientes códigos de error adicionales:

— Si no hay una clave pública presente en el entorno de seguridad, se devuelve '**6A88**'.

— Si no hay una clave privada presente en el entorno de seguridad, se contesta con el estado de procesado '**6A88**'.

— Si la verificación del criptograma es incorrecta, se contesta con el estado de procesado '**6688**'.

— Si se considera que la clave privada seleccionada está dañada, se contesta con el estado de procesado '**6400**' o '**6581**'.

La variante del comando para la autenticación de generación 2 puede devolver el siguiente código de error adicional:

— Si falla la verificación de la firma, la tarjeta contesta con el estado '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Este comando sirve para el protocolo de autenticación de chips de generación que se especifica en la parte B del apéndice 11 y cumple con lo dispuesto en la norma ISO/CEI 7816-4.

TCS_100 El comando puede ejecutarse en el MF, DF tacógrafo y DF tacógrafo_G2; véase también TCS_34TCS_34.

TCS_101 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Claves y protocolo conocidos implícitamente
P2	1	'00h'	
Lc	1	'NNh'	Lc: longitud del campo de datos subsiguiente
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Valor de clave pública efímera codificada con DER-TLV (véase el apéndice 11) La VU deberá enviar los objetos de datos en este orden.

TCS_102 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	Datos de autenticación dinámica codificados con DER-TLV: Testigo de autentificación específico (véase el apéndice 11)
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— La tarjeta contesta con el estado '**6A80**' para indicar parámetros incorrectos en el campo de datos.

— La tarjeta contesta con el estado '**6982**' si el comando de autenticación externa no se ha ejecutado correctamente.

El objeto de datos de autenticación dinámica de respuesta '7Ch'

— debe estar presente si la operación se realiza con éxito, es decir, las palabras de estado son '**9000**',

— debe estar ausente en caso de que se produzca un error de ejecución o un error de comprobación, es decir, si las palabras de estado se encuentran en el intervalo '**6400**' — '**6FFF**', y

— puede estar ausente en caso de que se produzca una advertencia, es decir, si las palabras de estado se encuentran en el intervalo '**6200**' — '**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Este comando se utiliza para determinar una clave pública con fines de autentificación.

3.5.11.1 Comando de generación 1 — Par de respuestas

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-4. Este comando tiene un uso restringido en relación con dicha norma.

TCS_103 Este comando es compatible únicamente con una aplicación de tacógrafo de generación 1.

TCS_104 La clave a que se hace referencia en el campo de datos MSE sigue siendo la clave pública actual hasta el siguiente comando MSE correcto, hasta que se selecciona un DF o hasta que se restablece la tarjeta.

TCS_105 Si la clave a que se hace referencia no está (ya) presente en la tarjeta, el entorno de seguridad no experimenta cambio alguno.

TCS_106 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: clave a que se hace referencia, válida para todas las operaciones criptográficas
P2	1	'B6h'	P2 (datos a que se hace referencia, relativos a la firma digital)
Lc	1	'0Ah'	Lc: longitud del campo de datos subsiguiente
#6	1	'83h'	Etiqueta para hacer referencia a una clave pública en casos asimétricos
#7	1	'08h'	Longitud de la referencia de la clave (identificador de clave)
#8-#15	8	'XX..XXh'	Identificador de clave según se especifica en el apéndice 11

TCS_107 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si la clave a que se hace referencia no está presente en la tarjeta, se contesta con el estado de procesado '**6A88**'.

— Si en el formato de mensajería segura faltan algunos de los objetos de datos que se esperaban, se devuelve el estado de procesado '**6987**'. Esto puede ocurrir si falta la etiqueta '83h'.

— Si algunos objetos de datos son incorrectos, se contesta con el estado de procesado '**6988**'. Esto puede ocurrir si la longitud del identificador de clave no es '08h'.

— Si se considera que la clave seleccionada está dañada, se contesta con el estado de procesado '**6400**' o '**6581**'.

3.5.11.2 Comando de generación 2 — Pares de respuestas

En cuanto a la autenticación de generación 2, la tarjeta de tacógrafo admite los siguientes MSE: Versiones de comando establecidas que cumplen la norma ISO/CEI 7816-4. Estas versiones de comando no son compatibles con la autenticación de generación 1.

3.5.11.2.1 MSE:SET AT para la autenticación del chip

El siguiente comando MSE:SET AT sirve para seleccionar los parámetros de autenticación del chip que se realiza mediante un comando de autenticación general subsiguiente.

TCS_108 El comando puede ejecutarse en el MF, DF tacógrafo y DF tacógrafo_G2; véase también TCS_34TCS_34.

TCS_109 **Mensaje del comando MSE:SET AT para la autenticación del chip**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'22h'	

Byte	Longitud	Valor	Descripción
P1	1	'41h'	Establecido para autenticación interna
P2	1	'A4h'	Autenticación
Lc	1	'NNh'	Lc: longitud del campo de datos subsiguiente
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Referencia del mecanismo criptográfico codificado con DER-TLV: Identificador de objetos de autenticación del chip (solo el valor, se omite la etiqueta '06h'). Véase el apéndice 1 para conocer los valores de los identificadores de objetos; se utilizará la notación en bytes. Véase el apéndice 11 para conocer las orientaciones sobre cómo seleccionar uno de estos identificadores de objetos.

3.5.11.2.2 MSE:SET AT para la autenticación de la VU

El siguiente comando MSE:SET AT sirve para seleccionar los parámetros y las claves de autenticación de la VU que se realiza mediante un comando de autenticación externa subsiguiente.

TCS_110 El comando puede ejecutarse en el MF, DF tacógrafo y DF tacógrafo_G2; véase también TCS_34TCS_34.

TCS_111 **Mensaje del comando MSE:SET AT para la autenticación de la VU**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Establecido para autenticación externa
P2	1	'A4h'	Autenticación
Lc	1	'NNh'	Lc: longitud del campo de datos subsiguiente
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Referencia del mecanismo criptográfico codificado con DER-TLV: Identificador de objetos de autenticación de la VU (solo el valor, se omite la etiqueta '06h'). Véase el apéndice 1 para conocer los valores de los identificadores de objetos; se utilizará la notación en bytes. Véase el apéndice 11 para conocer las orientaciones sobre cómo seleccionar uno de estos identificadores de objetos.
		'83h' + '08h' + 'XX..XXh'	Referencia codificada con DER-TLV de la clave pública de la VU por medio de la referencia al titular del certificado citado en el presente certificado.
		'91h' + L_{91} + 'XX..XXh'	Representación comprimida y codificada con DER-TLV de la clave pública efímera de la VU que se utilizará durante la autenticación del chip (véase el apéndice 11)

3.5.11.2.3 MSE:SET DST

El siguiente comando MSE:SET DST se utiliza para establecer una clave pública ya sea

— para la verificación de una firma suministrada en un PSO subsiguiente: el comando Verify Digital Signature, ya sea

— para la verificación de la firma de un certificado suministrado en un PSO subsiguiente: el comando Verify Certificate

TCS_112 El comando puede ejecutarse en el MF, DF tacógrafo y DF tacógrafo_G2; véase también TCS_33.

TCS_113 **Mensaje del comando MSE:SET DST**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Establecido para verificación
P2	1	'B6h'	Firma digital
Lc	1	'NNh'	Lc: longitud del campo de datos subsiguiente
#6-#(5+L)	L	'83h' + '08h' + 'XX...XXh'	Referencia codificada con DER-TLV de una clave pública, es decir, la referencia al titular del certificado en el certificado de la clave pública (véase el apéndice 11)

Para todas las versiones del comando, la estructura del mensaje de respuesta y las palabras de estado vienen dadas por:

TCS_114 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'. Se ha seleccionado e inicializado el protocolo.

— '**6A80**' indica parámetros incorrectos en el campo de datos del comando.

— '**6A88**' indica que los datos a que se hace referencia (es decir, una clave referenciada) no están disponibles.

3.5.12 *PSO: HASH*

Este comando sirve para transferir a la tarjeta el resultado de un cálculo de comprobación aleatoria con unos datos determinados. Este comando se utiliza para la verificación de firmas digitales. El valor de comprobación aleatoria se almacena temporalmente para el PSO del comando subsiguiente: Verify Digital Signature

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8. Este comando tiene un uso restringido en relación con dicha norma.

Solo la tarjeta de control debe admitir este comando en el DF tacógrafo y el DF tacógrafo_G2.

Otros tipos de tarjetas de tacógrafo pueden o no incorporar este comando. El comando puede o no estar accesible en el MF.

La aplicación de la tarjeta de control de generación 1 admite solo SHA-1.

TCS_115 El valor de comprobación aleatoria temporal deberá borrarse si se calcula un nuevo valor de comprobación aleatoria por medio del comando PSO: HASH si se selecciona un DF y si se reinicia la tarjeta del tacógrafo.

TCS_116 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'90h'	Devolver Hash code
P2	1	'A0h'	Etiqueta: campo de datos contiene DO relevantes para comprobación aleatoria
Lc	1	'XXh'	Longitud Lc del campo de datos subsiguiente
#6	1	'90h'	Etiqueta para el hash code
#7	1	'XXh'	Longitud L del hash code: '14h' en la aplicación generación 1 (véase la parte A del apéndice 11) '20h', '30h' o '40h' en la aplicación generación 2 (véase la parte B del apéndice 11)
#8-#(7+L)	L	'XX..XXh'	Hash code

TCS_117 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si faltan algunos de los objetos de datos que se esperaban (anteriormente especificados), se devuelve el estado de procesado '**6987**'. Esto puede ocurrir si falta una etiqueta '90h'.

— Si algunos objetos de datos son incorrectos, se contesta con el estado de procesado '**6988**'. Este error sucede si la etiqueta requerida está presente, pero tiene una longitud diferente desde '14h' para SHA-1, '20h' para SHA-256, '30h' para SHA-384, '40h' para SHA-512 (aplicación de generación 2).

3.5.13 *PERFORM HASH of FILE*

Este comando no cumple la norma ISO/CEI 7816-8. Por consiguiente, el byte CLA de este comando indica que hay un uso propio del comando PERFORM SECURITY OPERATION/HASH.

Solo la tarjeta del conductor y la tarjeta de taller deben admitir este comando en el DF tacógrafo y el DF tacógrafo_G2.

Otros tipos de tarjetas de tacógrafo pueden o no incorporar este comando. Si una tarjeta de empresa o de control incorpora este comando, el comando deberá aplicarse del modo especificado en el presente apartado.

El comando puede o no estar accesible en el MF. Si lo está, el comando deberá aplicarse del modo especificado en el presente apartado, es decir, no deberá permitir el cálculo de un valor de comprobación aleatoria, sino que terminará con un código de error adecuado.

TCS_118 El comando PERFORM HASH of FILE sirve para realizar una comprobación aleatoria en la zona de datos del EF transparente actualmente seleccionado.

TCS_119 Una tarjeta de tacógrafo deberá admitir este comando solo para los EF que se relacionan en el apartado 44 dentro del apartado del DF_tacógrafo y del DF_tacógrafo_G2 con la siguiente excepción. Una tarjeta de tacógrafo no deberá admitir el comando para el EF Sensor_Installation_Data del DF tacógrafo_G2.

TCS_120 El resultado de la operación de comprobación aleatoria se almacena temporalmente en la tarjeta. Posteriormente, puede utilizarse para obtener una firma digital del archivo por medio del PSO: el comando COMPUTE DIGITAL SIGNATURE.

TCS_121 El valor de comprobación aleatoria del archivo temporalmente almacenado deberá borrarse si se calcula un nuevo valor de comprobación aleatoria del archivo por medio del PSO: El comando «Hash of File», si se selecciona un DF y si se reinicia la tarjeta del tacógrafo.

TCS_122 La aplicación del tacógrafo de generación 1 deberá admitir SHA-1.

TCS_123 La aplicación del tacógrafo de generación 2 deberá admitir SHA-1 y SHA-2 (256, 384 y 512 bits).

TCS_124 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'80h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'90h'	Etiqueta: Hash
P2	1	'XXh'	P2: Indica el algoritmo que debe utilizarse para la comprobación aleatoria de los datos del archivo transparente seleccionado actualmente: '00h' para SHA-1 '01h' para SHA-256 '02h' para SHA-384 '03h' para SHA-512

TCS_125 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si el EF actual no admite este comando (EF Sensor_Installation_Data en DF tacógrafo_G2), se contesta con el estado de procesado '**6985**'.

— Si se considera que el EF seleccionado está dañado (errores de integridad en los atributos del archivo o los datos almacenados), se contesta con el estado de procesado '**6400**' o '**6581**'.

— Si el archivo seleccionado no es un archivo o si no existen ningún EF actual, se contesta con el estado de procesado '**6986**'.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Este comando sirve para calcular la firma digital de un código de comprobación aleatoria calculado previamente (véase PERFORM HASH of FILE, §3.5.133.5.13).

Solo la tarjeta del conductor y la tarjeta de taller deben admitir este comando en el DF tacógrafo y el DF tacógrafo_G2.

Otros tipos de tarjetas de tacógrafo pueden o no incorporar este comando, pero no tendrán una clave de firma. Por tanto, estas tarjetas no pueden ejecutar el comando correctamente, pero terminan con un código de error adecuado.

El comando puede o no estar accesible en el MF. En caso afirmativo, el comando deberá terminar con un código de error adecuado.

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8. Este comando tiene un uso restringido en relación con dicha norma.

TCS_126 Este comando no deberá calcular una firma digital del código de comprobación aleatoria calculado anteriormente con el comando PSO: HASH.

TCS_127 La tarjeta conoce implícitamente su clave privada, que se utiliza para calcular la firma digital.

TCS_128 La aplicación del tacógrafo de generación 1 realiza una firma digital utilizando un método de relleno conforme a la norma PKCS1 (véanse los detalles en el apéndice 11).

TCS_129 La aplicación del tacógrafo de generación 2 calcula una firma digital basada en una curva elíptica (véanse los detalles en el apéndice 11).

TCS_130 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'9Eh'	Firma digital que se ha de devolver
P2	1	'9Ah'	Etiqueta: el campo de datos contiene los datos que se han de firmar. Como se incluye ningún campo de datos, se supone que los datos ya están presentes en la tarjeta (comprobación aleatoria del archivo)
Le	1	'NNh'	Longitud de la firma esperada

TCS_131 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#L	L	'XX..XXh'	Firma de la comprobación aleatoria calculada previamente
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si se considera que la clave privada seleccionada implícitamente está dañada, se contesta con el estado de procesado '**6400**' o '**6581**'.

— Si el valor de comprobación aleatoria que fue calculado en un comando anterior Perform Hash of File no está disponible, se contesta con el estado de procesado '**6985**'.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Este comando sirve para verificar la firma digital, suministrada como entrada, cuya comprobación aleatoria conoce la tarjeta. La tarjeta conoce implícitamente el algoritmo de la firma.

Este comando cumple con lo dispuesto en la norma ISO/CEI 7816-8. Este comando tiene un uso restringido en relación con dicha norma.

Solo la tarjeta de control debe admitir este comando en el DF tacógrafo y el DF tacógrafo_G2.

Otros tipos de tarjetas de tacógrafo pueden o no incorporar este comando. El comando puede o no estar accesible en el MF.

TCS_132 El comando VERIFY DIGITAL SIGNATURE siempre utiliza la clave pública seleccionada por el Manage Security Environment (MSE) anterior: el comando Set DST y el código de comprobación aleatoria anterior introducido por un comando PSO: HASH.

TCS_133 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'00h'	CLA
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'00h'	
P2	1	'A8h'	Etiqueta: el campo de datos contiene DO relevantes para verificación
Lc	1	'83h'	Longitud Lc del campo de datos subsiguiente
6	1	'9Eh'	Etiqueta para firma digital
#7-#8	2	'81 XXh'	Longitud de la firma digital: 128 bytes codificados conforme a la parte A del apéndice 11 para una aplicación de tacógrafo de generación 1 Dependiendo de la curva seleccionada para la aplicación de tacógrafo de generación 2 (véase la parte B del apéndice 11)
#9-#(8+L)	L	'XX..XXh'	Contenido de la firma digital

TCS_134 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— Si la verificación de la firma falla, se contesta con el estado de procesado '**6688**'. El proceso de verificación se describe en el apéndice 11.

— Si no se selecciona una clave pública, se contesta con el estado de procesado '**6A88**'.

— Si faltan algunos de los objetos de datos que se esperaban (anteriormente especificados), se devuelve el estado de procesado '**6987**'. Esto puede ocurrir si falta una de las etiquetas necesarias.

— Si no hay disponible un código de comprobación aleatoria para procesar el comando (como resultado de un comando anterior PSO: comando HASH), se contesta con el estado de procesado '**6985**'.

— Si algunos objetos de datos son incorrectos, se contesta con el estado de procesado '**6988**'. Esto puede ocurrir si la longitud de uno de los objetos de datos necesarios es incorrecta.

— Si se considera que la clave pública seleccionada está dañada, se contesta con el estado de procesado '**6400**' o '**6581**'.

3.5.16 *PROCESS DSRC MESSAGE*

Este comando sirve para verificar la integridad y autenticidad del mensaje DSRC y para descifrar los datos transmitidos desde una VU a una autoridad de control o a un centro de ensayo a través del enlace DSRC. La tarjeta obtiene la clave de cifrado y la clave MAC utilizada para asegurar el mensaje DSRC del modo descrito en el apartado 13 de la parte B del apéndice 11.

Solo la tarjeta de control y la tarjeta de taller deben admitir este comando en el DF tacógrafo_G2.

Otros tipos de tarjetas de tacógrafo pueden o no incorporar este comando, pero no tendrán una clave maestra DSRC. Por tanto, estas tarjetas no pueden ejecutar el comando correctamente, pero terminan con un código de error adecuado.

El comando puede o no estar accesible en el MF y/o el DF tacógrafo. En caso afirmativo, el comando deberá terminar con un código de error adecuado.

TCS_135 La clave maestra DSRC es accesible únicamente en el DT tacógrafo_G2, es decir, la tarjeta de control y la de taller deberán admitir una ejecución correcta del comando solo en el DF tacógrafo_G2.

TCS_136 El comando deberá descifrar solamente los datos DSRC y verificar la suma de control criptográfica, pero sin interpretar los datos de entrada.

TCS_137 El orden de los objetos de datos en el campo de datos del comando queda fijado por la presente especificación.

TCS_138 **Mensaje de comando**

Byte	Longitud	Valor	Descripción
CLA	1	'80h'	CLA propio
INS	1	'2Ah'	Realizar operación de seguridad
P1	1	'80h'	Datos de respuesta: valor plano
P2	1	'B0h'	Datos del comando: valor plano codificado en BER-TLV e incluye SM DO
Lc	1	'NNh'	Longitud Lc del campo de datos subsiguiente
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Byte indicador del contenido de relleno codificado con DET-TLV seguido de los datos útiles cifrados del tacógrafo. Se utilizará el valor '00h' ('ninguna otra indicación' según la tabla 52 de la norma ISO/CIE 7816-4:2013) para el byte indicador del contenido de relleno. Véase el apartado 13 de la parte B del apéndice 11 para obtener más información sobre el mecanismo de cifrado. Los valores permitidos para la longitud L_{87} son múltiplos de la longitud del bloque AES más 1 para el byte indicador del contenido de relleno, es decir, desde 17 bytes hasta 193 bytes inclusive. *Nota:* Véase la tabla 49 de la norma ISO/CIE 7816-4:2013 para más información sobre el objeto de datos SM con etiqueta '87h'.
		'81h' + '10h'	Plantilla de la referencia de control para confidencialidad codificada con DER-TLV que anida la concatenación de los elementos de datos siguientes (véase el apéndice 1 DSRCSecurityData y el apartado 13 de la parte B del apéndice 11): — Indicación temporal de 4 bytes — Contador de 3 bytes — Número de serie de la VU de 8 bytes — Versión de la clave maestra DSRC de 1 byte *Nota:* Véase la tabla 49 de la norma ISO/CIE 7816-4:2013 para más información sobre el objeto de datos SM con etiqueta '81h'.
		'8Eh' + L_{8E} + 'XX..XXh'	MAC codificada con DER-TLV a través del mensaje DSRC. Véase el apartado 13 de la parte B del apéndice 11 para obtener más información sobre el algoritmo y cálculo de MAC. *Nota:* Véase la tabla 49 de la norma ISO/CIE 7816-4:2013 para más información sobre el objeto de datos SM con etiqueta '8Eh'.

TCS_139 **Mensaje de respuesta**

Byte	Longitud	Valor	Descripción
#1-#L	L	'XX..XXh'	Ausente (en caso de error) o datos descifrados (relleno eliminado)
SW	2	'XXXXh'	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, la tarjeta contesta con el estado '**9000**'.

— '**6A80**' indica parámetros incorrectos en el campo de datos del comando (también se utiliza en caso de que los objetos de datos no se envíen en el orden especificado).

— '**6A88**' indica que los datos a que se hace referencia, es decir, la clave maestra DSRC referenciada, no están disponibles.

— '**6900**' indica que ha fallado la verificación de la suma de control criptográfica o el descifrado de los datos.

4. ESTRUCTURA DE LAS TARJETAS DE TACÓGRAFO

El presente apartado especifica las estructuras de archivos de las tarjetas de tacógrafo para el almacenamiento de datos accesibles.

No se especifican las estructuras internas que dependen del fabricante de la tarjeta, como por ejemplo las cabeceras de archivos, ni el almacenamiento y la manipulación de elementos de datos necesarios para uso interno exclusivamente, como `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` o `WorkshopCardPin`.

TCS_140 Una tarjeta de tacógrafo de generación 2 deberá incorporar el archivo maestro MF y una aplicación de tacógrafo de generación 1 y de generación 2 del mismo tipo (por ejemplo, aplicaciones de tarjeta del conductor).

TCS_141 Una tarjeta de tacógrafo deberá admitir al menos el número mínimo de registros especificados para las aplicaciones correspondientes y no admitirá más registros que el número máximo de registros especificados para las aplicaciones correspondientes.

Los números máximo y mínimo de registros se especifican en este apartado para las distintas aplicaciones.

En cuanto a las condiciones de seguridad utilizadas en las normas de acceso a lo largo de este apartado, véase el apartado 3.33.3. En general, el modo de acceso de «lectura» denota el comando READ BINARY con byte INS par y, si se admite, impar a excepción del EF Sensor_Installation_Data en la tarjeta de taller; véase TCS_156TCS_156 y TCS_160TCS_160. El modo de acceso de «actualización» denota el comando Update Binary con byte INS par y, si se admite, impar y el modo de acceso de «selección», el comando SELECT.

4.1. Archivo maestro MF

TCS_142 Una vez personalizado el archivo maestro MF, tendrá la siguiente estructura permanente de archivo y las normas de acceso al archivo:

Nota: .El identificador EF corto SFID se da como número decimal, por ejemplo, el valor 30 se corresponde con 11110 en binario.

			Normas de acceso	
Archivo	**ID del archivo**	**SFID**	**Leer / Seleccionar**	**Actualización**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

En esta tabla se utiliza la siguiente abreviación para la condición de seguridad:

SC1 ALW OR SM-MAC-G2

TCS_143 La estructura de todos los EF deberá ser transparente.

TCS_144 El archivo principal (MF) deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
MF		*63*	*164*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 El archivo elemental EF DIR deberá contener los siguientes objetos de datos relacionados con la aplicación: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 El archivo elemental EF ATR/INFO deberá estar presente si la tarjeta de tacógrafo indica en su ATR que admite campos de longitud ampliada. En este caso, el EF ATR/INFO llevará el objeto de datos con información de longitud ampliada (DO'7F66') tal como se especifica en la cláusula 12.7.1 de la norma ISO/CIE 7816-4:2013.

TCS_147 El archivo elemental EF Extended_Length deberá estar presente si la tarjeta de tacógrafo indica en su ATR que admite campos de longitud ampliada. En este caso, el EF contendrá el siguiente objeto de datos: '02 01 xx', donde el valor 'xx' indica si se admiten campos de longitud extendida para el protocolo T = 1 y/o T = 0.

El valor '01' indica compatibilidad con el campo de longitud extendida para el protocolo T = 1.

El valor '10' indica compatibilidad con el campo de longitud extendida para el protocolo T = 0.

El valor '11' indica compatibilidad con el campo de longitud extendida para el protocolo T = 1 y el T = 0.

4.2. Aplicaciones de la tarjeta del conductor

4.2.1 *Aplicación de la tarjeta de conductor de generación 1*

TCS_148 Una vez personalizada, la aplicación de la tarjeta de conductor de generación 1 tendrá la siguiente estructura permanente de archivos y las normas de acceso a los archivos:

File	ID del archivo	Normas de acceso		
		Leer	Seleccionar	Actualización
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'050Eh'	SC2	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

En esta tabla se utilizan las siguientes abreviaciones para las condiciones de seguridad:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 La estructura de todos los EF deberá ser transparente.

TCS_150 La aplicación de generación 1 de la tarjeta de conductor deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*2604*	*6200*	
└─CardVehicleRecord	n_3	*31*	*31*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*840*	*1120*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_151 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de conductor debe utilizar para una aplicación de generación 1:

		Min	Max
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 días * 93 cambios de actividad)	13 776 bytes (28 días * 240 cambios de actividad)

4.2.2 *Aplicación de la tarjeta de conductor de generación 2*

TCS_152 Una vez personalizada, la aplicación de la tarjeta de conductor de generación 2 tendrá la siguiente estructura permanente de archivos y las normas de acceso a los archivos.

Nota: .El identificador EF corto SFID se da como número decimal, por ejemplo, el valor 30 se corresponde con 11110 en binario.

			Normas de acceso	
File	**ID del archivo**	**SFID**	**Leer / Seleccionar**	**Actualización**
└─ DF Tachograph_G2			SC1	
├─ EF Application_Identification	'0501h'	1	SC1	NEV
├─ EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─ EF CardSignCertificate	'C101h'	3	SC1	NEV
├─ EF CA_Certificate	'C108h'	4	SC1	NEV
├─ EF Link_Certificate	'C109h'	5	SC1	NEV
├─ EF Identification	'0520h'	6	SC1	NEV
├─ EF Card_Download	'050Eh'	7	SC1	SC1
├─ EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─ EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─ EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─ EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─ EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─ EF Places	'0506h'	16	SC1	SM-MAC-G2
├─ EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─ EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─ EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─ EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─ EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

En esta tabla se utiliza la siguiente abreviación para la condición de seguridad:

SC1 ALW OR SM-MAC-G2

TCS_153 La estructura de todos los EF deberá ser transparente.

TCS_154 La aplicación de generación 2 de la tarjeta de conductor deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (bytes) Min	Max	Default Values
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
CardVehiclesUsed		*4034*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*4032*	*9600*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
CardPlaceDailyWorkPeriod		*1766*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*1764*	*2352*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo de los números de registro que la estructura de datos de la tarjeta de conductor debe utilizar para una aplicación de generación 2:

		Min	**Max**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 días * 93 cambios de actividad)	13 776 bytes (28 días * 240 cambios de actividad)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Aplicaciones de la tarjeta de taller

4.3.1 *Aplicación de la tarjeta del centro de ensayo de generación 1*

TCS_156 Una vez personalizada, la aplicación de la tarjeta de taller de generación 1 tendrá la siguiente estructura permanente de archivos y las normas de acceso a los archivos:

		Access rules		
File	**File ID**	**Read**	**Select**	**Update**
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'0509h'	SC2	SC1	**SC1**
├─EF Calibration	'050Ah'	SC2	SC1	SC3
├─EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

En esta tabla se utilizan las siguientes abreviaciones para las condiciones de seguridad:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 Para el comando READ BINARY con byte INS par:

(PLAIN-C AND SM-R-ENC-G1) O (SM-C-MAC-G1 Y SM-R-ENC-MAC-G1) O

(SM-C-MAC-G2 Y SM-R-ENC-MAC-G2)

Para el comando READ BINARY con byte INS impar (si se admite): NEV

TCS_157 La estructura de todos los EF deberá ser transparente.

TCS_158 La aplicación de la tarjeta de taller de generación 1 deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (Bytes) Min	Size (Bytes) Max	Default Values
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
└CardPlaceDailyWorkPeriod		*61*	*81*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*60*	*80*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de taller debe utilizar para una aplicación de generación 1:

		Min	**Max**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 día * 93 cambios de actividad)	492 bytes (1 día * 240 cambios de actividad)

4.3.2 *Aplicación de la tarjeta de taller de generación 2*

TCS_160 Una vez personalizada, la aplicación de la tarjeta de taller de generación 2 tendrá la siguiente estructura permanente de archivos y las normas de acceso a los archivos.

Nota: .El identificador EF corto SFID se da como número decimal, por ejemplo, el valor 30 se corresponde con 11110 en binario.

			Access rules		
File	**File ID**	**SFID**	**Read**	**Select**	**Update**
└DF Tachograph_G2			SC1	SC1	
├EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├EF Identification	'0520h'	6	SC1	SC1	NEV
├EF Card_Download	'0509h'	7	SC1	SC1	SC1
├EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
├EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
└EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

En esta tabla se utilizan las siguientes abreviaciones para las condiciones de seguridad:

SC1 ALW OR SM-MAC-G2

SC5 Para el comando Read Binary con byte INS par: SM-C-MAC-G2 Y SM-R-ENC-MAC-G2

Para el comando Read Binary con byte INS impar (si se admite): NEV

TCS_161 La estructura de todos los EF deberá ser transparente.

TCS_162 La aplicación de la tarjeta de taller de generación 2 deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (Bytes) Min	Size (Bytes) Max	Default Values
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

├─oldTimeValue		4	4	{00..00}
├─newTimeValue		4	4	{00..00}
├─nextCalibrationDate		4	4	{00..00}
├─vuPartNumber		16	16	{20..20}
├─vuSerialNumber		8	8	{00..00}
├─sensorSerialNumber		8	8	{00..00}
├─sensorGNSSSerialNumber		8	8	{00..00}
├─rcmSerialNumber		8	8	{00..00}
├─vuAbility		1	1	{00}
└─sealDataCard		46	46	
├─noOfSealRecords		1	1	{00}
└─SealRecords		45	45	
└─SealRecord	5	9	9	
├─equipmentType		1	1	{00}
└─extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
└─SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
└─CardEventData		*792*	*792*	
└─cardEventRecords	11	*72*	*72*	
└─CardEventRecord	n_1	*24*	*24*	
├─eventType		1	1	{00}
├─eventBeginTime		4	4	{00..00}
├─eventEndTime		4	4	{00..00}
└─eventVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└─CardFaultData		*288*	*288*	
└─cardFaultRecords	2	*144*	*144*	
└─CardFaultRecord	n_2	*24*	*24*	
├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└─CardDriverActivity		*202*	*496*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
└─CardVehiclesUsed		*194*	*386*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*192*	*384*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

TCS_163 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de taller debe utilizar para una aplicación de generación 2:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 día * 93 cambios de actividad)	492 bytes (1 día * 240 cambios de actividad)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Aplicaciones de la tarjeta de control

4.4.1 *Aplicación de la tarjeta de control de generación 1*

TCS_164 Una vez personalizada, la aplicación de la tarjeta de control de generación 1 tendrá la siguiente estructura permanente de archivos y las normas de acceso a los archivos:

		Access rules		
File	**File ID**	**Read**	**Select**	**Update**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

En esta tabla se utilizan las siguientes abreviaciones para las condiciones de seguridad:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 O SM-MAC-G1 O SM-MAC-G2

TCS_165 La estructura de todos los EF deberá ser transparente.

TCS_166 La aplicación de la tarjeta de control de generación 1 deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (Bytes) Min	Max	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de control debe utilizar para una aplicación de generación 1:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Aplicación de la tarjeta de control de generación 2*

TCS_168 Una vez personalizada, la aplicación de la tarjeta de control de generación 2 tendrá la siguiente estructura permanente de archivos y las normas de acceso a los archivos:

Nota: .El identificador EF corto SFID se da como número decimal, por ejemplo, el valor 30 se corresponde con 11110 en binario.

			Access rules	
File	**File ID**	**SFID**	**Read / Select**	**Update**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

En esta tabla se utiliza la siguiente abreviación para la condición de seguridad:

SC1 ALW OR SM-MAC-G2

TCS_169 La estructura de todos los EF deberá ser transparente.

TCS_170 La aplicación de la tarjeta de control de generación 2 deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (Bytes) Min	Max	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de control debe utilizar para una aplicación de generación 2:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.5. Aplicaciones de la tarjeta de empresa

4.5.1 *Aplicación de la tarjeta de empresa de generación 1*

TCS_172 Una vez personalizada, la aplicación de la tarjeta de empresa de generación 1 tendrá la siguiente estructura permanente de archivos y las normas de acceso a los archivos:

File	File ID	Access rules		
		Read	Select	Update
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	**SC6**	SC1	NEV
EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

En esta tabla se utilizan las siguientes abreviaciones para las condiciones de seguridad:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 O SM-MAC-G1 O SM-MAC-G2

TCS_173 La estructura de todos los EF deberá ser transparente.

TCS_174 La aplicación de la tarjeta de empresa de generación 1 deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph		*11114*	*24454*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_175 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de empresa debe utilizar para una aplicación de generación 1:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Aplicación de la tarjeta de empresa de generación 2*

TCS_176 Una vez personalizada, la aplicación de la tarjeta de empresa de generación 2 tendrá la siguiente estructura permanente de archivos y las normas de acceso a los archivos.

Nota: .El identificador EF corto SFID se da como número decimal, por ejemplo, el valor 30 se corresponde con 11110 en binario.

			Access rules	
File	**File ID**	**SFID**	**Read / Select**	**Update**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

En esta tabla se utiliza la siguiente abreviación para la condición de seguridad:

SC1 ALW OR SM-MAC-G2

TCS_177 La estructura de todos los EF deberá ser transparente.

TCS_178 La aplicación de la tarjeta de empresa de generación 2 deberá tener la siguiente estructura de datos:

File / Data element	No of Records	Size (bytes) Min	Max	Default Values
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 Los valores siguientes, empleados para indicar tamaños en la tabla anterior, son los valores máximo y mínimo que la estructura de datos de la tarjeta de empresa debe utilizar para una aplicación de generación 2:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

Apéndice 3

PICTOGRAMAS

PIC_001 El tacógrafo podrá utilizar, de forma opcional, los siguientes pictogramas y combinaciones de pictogramas (o pictogramas y combinaciones lo suficientemente parecidas para identificarse con estas de forma inequívoca):

1. PICTOGRAMAS BÁSICOS

	Personas	**Acciones**	**Modos de funcionamiento**
	Empresa		Modo de empresa
	Controlador	Control	Modo de control
	Conductor	Conducción	Modo operativo
	Taller/centro de ensayo	Inspección/calibrado	Modo de calibrado
	Fabricante		
	Actividades	**Duración**	
	Disponible	Período de disponibilidad actual	
	Conducción	Tiempo de conducción continua	
	Descanso	Período de descanso actual	
	Otro trabajo	Período de trabajo actual	
	Pausa	Tiempo de pausa acumulado	
	Indeterminado		
	Equipo	**Funciones**	
1	Ranura del conductor		
2	Ranura del segundo conductor		
	Tarjeta		
	Reloj		
	Pantalla	Visualización	
	Almacenamiento externo	Transferencia	
	Fuente de alimentación		
	Impresora/doc. impreso	Impresión	
	Sensor		
	Tamaño de los neumáticos		
	Vehículo/unidad instalada en el vehículo		
	Dispositivo GNSS		
	Dispositivo de detección a distancia		
	Interfaz STI		
	Condiciones específicas		
OUT	Fuera de ámbito		
	Trayecto en transbordador/tren		

Varios

!	Incidentes	⤫	Fallos
⏵	Comienzo del período de trabajo diario	⏵|	Final del período de trabajo diario
●	Lugar		
M	Entrada manual de las actividades del conductor		
🔒	Seguridad		
>	Velocidad		
🕒	Hora		
Σ	Total/resumen		

Calificadores

24h	Diario
|	Semanal
||	Bisemanal
✚	Desde o hasta

2. COMBINACIONES DE PICTOGRAMAS

Varios

🏛●	Lugar de control		
●⏵	Lugar donde comienza el período de trabajo diario	⏵|●	Lugar donde termina el período de trabajo diario
🕒✚	Hora de comienzo	✚🕒	Hora de conclusión
🚙✚	Desde el vehículo		
OUT✚	Comienzo condición Fuera de ámbito	✚OUT	Final condición Fuera de ámbito

Tarjetas

👤💳	Tarjeta de conductor
🏢💳	Tarjeta de empresa
🏛💳	Tarjeta de control
🔧💳	Tarjeta de taller
💳– – –	Sin tarjeta

Conducción

👤👤	Conducción en equipo
👤|	Tiempo de conducción en una semana
👤||	Tiempo de conducción en dos semanas

Documentos impresos

24h 💳🖨	Impresión diaria de las actividades del conductor almacenadas en la tarjeta
24h 🚙🖨	Impresión diaria de las actividades del conductor almacenadas en la VU
!⤫💳🖨	Impresión de incidentes y fallos almacenados en la tarjeta
!⤫🚙🖨	Impresión de incidentes y fallos almacenados en la VU
🔧🕒🖨	Impresión de datos técnicos
>>🖨	Impresión de excesos de velocidad

Incidentes

	Inserción de una tarjeta no válida
	Conflicto de tarjetas
	Solapamiento temporal
	Conducción sin tarjeta adecuada
	Inserción de tarjeta durante la conducción
	Error al cerrar la última sesión de la tarjeta
	Exceso de velocidad
	Interrupción del suministro eléctrico
	Error en datos de movimiento
	Conflicto de movimiento del vehículo
	Violación de la seguridad
	Ajuste de la hora (por el taller)
	Control del exceso de velocidad

Fallos

	Fallo de tarjeta (ranura del conductor)
	Fallo de tarjeta (ranura del segundo conductor)
	Fallo de la pantalla
	Fallo de transferencia
	Fallo de la impresora
	Fallo del sensor
	Fallo interno de la VU
	Fallo del dispositivo GNSS
	Fallo de la detección a distancia

Procedimiento de entrada manual

	¿Continúa el mismo período de trabajo diario?
	¿Final del anterior período de trabajo?
	Confirme o introduzca el lugar donde termina el período de trabajo
	Introduzca la hora de comienzo
	Introduzca el lugar donde comienza el período de trabajo

Nota: En el apéndice 4 se definen otras combinaciones de pictogramas que representan bloques de impresión o identificadores de registro.

Apéndice 4

DOCUMENTOS IMPRESOS

ÍNDICE

1. GENERALIDADES

Cada documento impreso es una concatenación de varios bloques de datos, posiblemente identificados con un identificador de bloque.

Un bloque de datos contiene uno o más registros, posiblemente identificados con un identificador de registro.

PRT_001 Cuando un identificador de bloque precede inmediatamente a un identificador de registro, el identificador de registro no se imprime.

PRT_002 Cuando una unidad de información se desconoce o no debe imprimirse por motivos relacionados con los derechos de acceso a los datos, en su lugar se imprimen espacios.

PRT_003 Si el contenido de una línea entera es desconocido o no tiene que imprimirse, se omite toda la línea.

PRT_004 Los campos de datos numéricos se imprimen alineados a la derecha, con un espacio como separador de las unidades de millar y de millón, y sin ceros a la izquierda.

PRT_005 Los campos de datos en cadena se imprimen alineados a la izquierda. Cuando es preciso (en nombres y direcciones), se rellenan con espacios hasta alcanzar la longitud de la unidad de información, o bien se truncan para no sobrepasar dicha longitud.

PRT_006 Cuando haya que dividir una línea cuyo texto sea largo, debe imprimirse un carácter especial (un punto a media altura de la línea, «•») como primer carácter en la línea nueva.

2. ESPECIFICACIÓN DE LOS BLOQUES DE DATOS

En este capítulo se han utilizado las siguientes convenciones para la notación de formatos:

— los caracteres impresos en **negrita** indican texto legible que hay que imprimir (en caracteres normales),

— los caracteres normales indican variables (pictogramas o datos) que hay que sustituir por sus valores antes de proceder a la impresión,

— los nombres de las variables se han acabado de llenar con guiones bajos con el fin de mostrar la longitud disponible para la variable en ese elemento de información,

— las fechas se especifican con el formato «dd/mm/aaaa» (día, mes, año). También se puede utilizar el formato «dd.mm.aaaa»,

— el término «identificación de la tarjeta» indica la composición de: el tipo de tarjeta (mediante una combinación de pictogramas), el código del Estado miembro que ha expedido la tarjeta, un carácter de barra oblicua y el número de tarjeta con el índice de sustitución y el índice de renovación separados por espacios:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Combinaciones de pictogramas de tarjeta		Código del Estado miembro emisor				Primeros 14 caracteres del número de tarjeta (incluido posiblemente un índice consecutivo)														Índice de sustitución		Índice de renovación

PRT_007 Los documentos impresos deberán utilizar los siguientes bloques de datos y/o registros de datos, con arreglo a los significados y formatos que se exponen a continuación:

Número de bloque o de registro Significado	Data Format
1 ***Fecha y hora en la que se imprime el documento.***	▼ dd/mm/aaaa hh:mm **(UTC)**
2 ***Tipo de documento impreso.*** Identificador del bloque Combinación de pictogramas en el documento (véase el apéndice 3), valor de ajuste del dispositivo limitador de la velocidad (impresión únicamente en caso de exceso de velocidad)	----------▼---------- Picto xxx **km/h**
3 ***Identificación del titular de la tarjeta*** Identificador del bloque. P = pictograma de persona Apellido(s) del titular de la tarjeta Nombre del titular de la tarjeta (si procede) Identificación de la tarjeta Fecha de caducidad de la tarjeta (en su caso) y número de generación de tarjeta (GEN 1 o GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/aaaa - GEN 2

Si se trata de una tarjeta no personal o no figura el apellido del titular de la misma, se imprimirá en su lugar el nombre de la empresa, del taller o del organismo de control.

(*) El número de generación de tarjeta solo puede imprimirlo el tacógrafo inteligente.

4 ***Identificación de los vehículos.*** Identificador del bloque VIN Estado miembro de matriculación y VRN	----------🚘---------- 🚘 VIN_____ Nat/VRN_____
5 ***Identificación de la unidad instalada en el vehículo (VU).*** Identificador del bloque Nombre del fabricante de la VU Número de pieza de la VU Número de generación de la VU (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) El número de generación de tarjeta solo puede imprimirlo el tacógrafo inteligente.

6 ***Último calibrado del tacógrafo*** Identificador del bloque Nombre del taller Identificación de la tarjeta de taller Fecha del calibrado	----------🔧---------- 🔧 Last_Name_____ Card_Identification_____ 🔧 dd/mm/aaaa

7 ***Último control (efectuado por un controlador)***

Identificador del bloque
Identificación de la tarjeta del controlador
Fecha, hora y tipo de control

```
----------▯----------
Card_Identification_____
▯ dd/mm/aaaa hh:mm ppppp
```

Tipo de control: máximo cinco pictogramas. El tipo de control puede consistir en (una combinación de):

▬: Transferencia o descarga de los datos de la tarjeta, ▼: descarga de la VU, ▛: impresión, ▯: visualización, ⊤: comprobación del calibrado en carretera

8 ***Actividades del conductor almacenadas en una tarjeta por orden de ocurrencia***

Identificador del bloque
Fecha de petición (día natural objeto de impresión) + Contador de presencias diarias de la tarjeta

```
----------⊙----------
    dd/mm/aaaa  xxx
```

8a *Condición fuera de ámbito al comienzo del presente día* (dejar en blanco si no hay condición fuera de ámbito abierta)

```
----------FUERA----------
```

8,1 *Intervalo de tiempo sin introducir la tarjeta*

8.1a Identificador de registro (comienzo del intervalo)
8.1b *Intervalo desconocido*. Hora de inicio, duración
8.1c *Actividad introducida manualmente*.
Pictograma de la actividad, hora de inicio, duración

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Introducción de la tarjeta en la ranura S*

Identificador de registro; S = Pictograma de ranura
Estado miembro de matriculación del vehículo y VRN
Lectura del cuentakilómetros del vehículo al introducir la tarjeta

```
  ---------S---------
▲ Nat/VRN__________
  x xxx xxx km
```

8.3 *Actividad (permaneciendo introducida la tarjeta)*

Pictograma de la actividad, hora de inicio, duración, estado del equipo (pictograma del equipo en modalidad EQUIPO; dejar en blanco en modalidad SOLITARIO).

```
A       hh:mm hhhmm ⊙⊙
```

8.3a *Condición específica*. Hora de entrada, pictograma de la condición específica (o combinación de pictogramas).

```
        hh:mm ---pppp---
```

8.4 *Extracción de la tarjeta*

Lectura del cuentakilómetros del vehículo y distancia recorrida desde la última introducción de cuyo valor se dispone

```
  x xxx xxx km; x xxx km
```

9 ***Actividades del conductor almacenadas en una VU por ranura y por orden cronológico***

Identificador del bloque
Fecha de petición (día del calendario objeto de impresión)
Lectura del cuentakilómetros del vehículo a las 00:00 y a las 24:00 horas

```
----------⊙----------
       dd/mm/aaaa
x xxx xxx - x xxx xxx km
```

10 ***Actividades realizadas en la ranura S***

Identificador del bloque

```
----------S----------
```

10a *Condición fuera de ámbito al comienzo del presente día* (dejar en blanco si no hay condición fuera de ámbito abierta)

```
----------FUERA----------
```

10.1 *Intervalo sin que haya una tarjeta introducida en la ranura S*

Identificador de registro.
Ninguna tarjeta introducida
Lectura del cuentakilómetros del vehículo al comienzo del intervalo

```
  --------------------
⊙▬---
  x xxx xxx km
```

10.2 *Introducción de la tarjeta*

Identificador de registro de introducción de la tarjeta
Apellido(s) del conductor

```
  --------------------
⊙ Apellido(s)_____________
```

	Nombre del conductor	First_Name_____
	Identificación de la tarjeta del conductor	Card_Identification_____
	Fecha de caducidad de la tarjeta (en su caso) y número de generación de tarjeta (GEN 1 o GEN 2) (*)	dd/mm/aaaa - GEN 2
	Estado miembro de matriculación y VRN del vehículo previo utilizado	País/VRN_____
	Fecha y hora de extracción de la tarjeta del vehículo previo	dd/mm/aaaa hh:mm
	Línea en blanco	
	Lectura del cuentakilómetros del vehículo al insertar la tarjeta, bandera indicativa de la introducción manual de actividades del conductor (M en caso afirmativo; dejar en blanco en caso negativo). Si no ha habido inserción de la tarjeta de conductor el día en que tiene lugar la impresión, se utilizará en el bloque 10.2 la lectura del cuentakilómetros de la última inserción de la tarjeta disponible antes de ese día.	x xxx xxx **km** M
10.3	*Actividad*	
	Pictograma de la actividad, hora de inicio, duración, estado del equipo (pictograma del equipo en modalidad EQUIPO; dejar en blanco en modalidad SOLITARIO).	A hh:mm hh**h**mm ⊙⊙
10.3a	*Condición específica*. Hora de entrada, pictograma de la condición específica (o combinación de pictogramas).	hh:mm ---pppp---
10.4	*Extracción de la tarjeta o finalización del intervalo «Ninguna tarjeta introducida»*	
	Lectura del cuentakilómetros del vehículo al extraer la tarjeta o al finalizar el intervalo «Ninguna tarjeta introducida» y distancia recorrida desde su introducción, o bien desde el comienzo del intervalo «Ninguna tarjeta introducida».	x xxx xxx **km**; x xxx **km**

(*) El número de generación de tarjeta solo puede imprimirlo el tacógrafo inteligente.

11	***Resumen diario***	
	Identificador del bloque	----------Σ----------
11.1	***Resumen de la VU para los intervalos sin tarjeta en la ranura del conductor***	
	Identificador del bloque	1⊙▪---
11.2	***Resumen de la VU para los intervalos sin tarjeta en la ranura del segundo conductor***	
	Identificador del bloque	2⊙▪---
11.3	***Resumen diario de la UV para las actividades por conductor***	
	Identificador de registro	----------
	Apellido(s) del conductor	⊙ Last_Name_____
	Nombre del conductor	First_Name_____
	Identificación de la tarjeta del conductor	Card_Identification_____
11.4	*Introducción de los lugares donde comienzan o terminan los períodos de trabajo diarios*	
	pi=pictograma del lugar de comienzo/ finalización, hora, país y región	pihh:mm Cou Reg
	Cuentakilómetros	x xxx xxx **km**
11.5	*Introducción de los lugares donde comienzan o terminan los períodos de trabajo diarios*	
	y después de un tiempo de conducción continua de tres horas	⁘ hh:mm
	Cuentakilómetros	x xxx xxx **km**
11.6	*Totalidad de actividades (extraídas de una tarjeta)*	
	Duración total del tiempo de conducción y distancia recorrida	⊙ hh**h**mm x xxx **km**
	Duración total de los períodos de trabajo y disponibilidad	⚒ hh**h**mm ⧈ hh**h**mm
	Duración total de los períodos de descanso y períodos indeterminados	⊢ hh**h**mm ? hh**h**mm
	Duración total de las actividades de equipo	⊙⊙ hh**h**mm
11.7	*Totalidad de actividades (intervalos sin tarjeta en la ranura del conductor)*	
	Duración total del tiempo de conducción y distancia recorrida	⊙ hh**h**mm x xxx **km**
	Duración total de los períodos de trabajo y disponibilidad	⚒ hh**h**mm ⧈ hh**h**mm
	Duración total de los períodos de descanso	⊢ hh**h**mm

11.8 *Totalidad de actividades (intervalos sin tarjeta en la ranura del segundo conductor)*

Duración total de los períodos de trabajo y disponibilidad	⚒ hh**h**mm ⧈ hh**h**mm
Duración total de los períodos de descanso	⊢ hh**h**mm

11.9 *Totalidad de actividades (por conductor, incluidas ambas ranuras)*

Duración total del tiempo de conducción y distancia recorrida	⊙ hh**h**mm x xxx **km**
Duración total de los períodos de trabajo y disponibilidad	⚒ hh**h**mm ⧈ hh**h**mm
Duración total de los períodos de descanso	⊢ hh**h**mm
Duración total de las actividades de equipo	⊙⊙ hh**h**mm

Cuando sea necesaria la impresión diaria de las actividades del día actual, el resumen diario de la información se hará a partir de los datos disponibles en el momento de la impresión.

12 ***Incidentes y/o fallos almacenados en la tarjeta Identificador del bloque:***

12.1	Identificador del bloque: últimos 5 «Incidentes y fallos» almacenados en la tarjeta	----------!×▪----------
12.2	Identificador del bloque: totalidad de «Incidentes» almacenada en la tarjeta	----------!▪----------
12.3	Identificador del bloque: totalidad de «Fallos» almacenada en la tarjeta	----------×▪----------

12.4 *Registro de incidentes y/o fallos*

Identificador de registro	----------
Pictograma de incidente/fallo, objeto del registro, fecha y hora de inicio del incidente/fallo	Pic (p) dd/mm/aaaa hh:mm
Código adicional indicativo del incidente/fallo (en su caso), duración	!xx hh**h**mm
Estado miembro de matriculación y VRN del vehículo en el que se haya producido el incidente/fallo	🚗 Nat/VRN_____

13 ***Incidentes y/o fallos almacenados o en curso en la VU Identificador del bloque:***

13.1	Identificador del bloque: últimos 5 «Incidentes y fallos» almacenados en la VU	----------!×🚗----------
13.2	Identificador del bloque: totalidad de «Incidentes» almacenados o en curso en la VU	----------!🚗----------
13.3	Identificador del bloque: totalidad de «Fallos» almacenados o en curso en la VU	----------×🚗----------

13.4 *Registro de incidentes y/o fallos*

Identificador de registro	----------
Pictograma de incidente/fallo, objeto del registro, fecha y hora de inicio del incidente/fallo	Pic (p) dd/mm/aaaa hh:mm
Código adicional indicativo del incidente/fallo (en su caso), número de incidentes análogos el mismo día, duración	!xx (xxx) hh**h**mm
Identificación de las tarjetas introducidas al comenzar o finalizar el incidente o fallo (máx. 4 líneas sin repetir dos veces los mismos números de tarjeta)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
Casos en que no hubiese tarjeta alguna introducida	▪---
Datos específicos del fabricante	< Literal><ErrorCode>

El registro tiene por objeto (p) un código numérico que explica el porqué del registro del incidente o fallo, codificado con arreglo al elemento de datos `EventFaultRecordPurpose`.

El `Literal` es un literal específico del fabricante del tacógrafo formado por un máximo de 12 caracteres.

El `ErrorCode` es un código de error específico del fabricante del tacógrafo formado por un máximo de 12 caracteres.

14 ***Identificación de la VU***

Identificador del bloque	----------B----------
Nombre del fabricante de la VU	B Name_____
Dirección del fabricante de la VU	Address_____
Número de pieza de la VU	PartNumber_____
Número de homologación de la VU	Apprv_____
Número de serie de la VU	S/N_____
Año de fabricación de la VU	aaaa
Fecha de instalación y versión del software de la VU	V xxxx dd/mm/aaaa

15 ***Identificación del sensor***

Identificador del bloque	----------J----------
15.1 *Registro de emparejamiento*	
Número de serie del sensor	J S/N_____
Número de homologación del sensor	Apprv_____
Fecha del emparejamiento del sensor	dd/mm/aaaa hh:mm

16 ***Identificación de GNSS***

Identificador del bloque	----------  ----------
16.1 *Registro de acoplamiento*	
Número de serie del dispositivo GNSS externo	 S/N_____
Número de homologación del dispositivo GNSS externo	Apprv_____
Número de acoplamiento del dispositivo GNSS externo	dd/mm/aaaa hh:mm

17 ***Datos de calibrado***

Identificador del bloque	----------T----------
17.1 *Registro de calibrado*	
Identificador de registro	----------
Taller que ha realizado el calibrado	T Workshop_name_____
Dirección del taller	Workshop_address_____
Identificación de la tarjeta de taller	Card_Identification_____
Fecha de caducidad de la tarjeta de taller	dd/mm/aaaa
Línea en blanco	
Fecha de calibrado + finalidad del calibrado	T dd/mm/aaaa (p)
VIN	A VIN_____
Estado miembro de matriculación y VRN	Nat/VRN_____
Coeficiente característico del vehículo	w xx xxx Imp/km
Constante del aparato de control	k xx xxx Imp/km
Effective circumference of wheel tyres	l xx xxx mm
Tamaño de los neumáticos instalados	● TyreSize_____
Valor de ajuste del dispositivo limitador de la velocidad	> xxx km/h
Lectura anterior y nueva lectura del cuentakilómetros	x xxx xxx – x xxx xxx km

El calibrado tiene por objeto (p) un código numérico que explica el porqué del registro de estos parámetros de calibrado, codificado con arreglo al elemento de datos `CalibrationPurpose`.

18 ***Ajuste de la hora***

	Identificador del bloque	----------◷----------
18.1	*Registro del ajuste de hora*	
	Identificador de registro	----------
	Fecha y hora anteriores	!◷ dd/mm/aaaa hh:mm
	Fecha y hora nuevas	◷ dd/mm/aaaa hh:mm
	Taller que ha realizado el ajuste de hora	⍑ Workshop_name_____
	Dirección del taller	Workshop_address_____
	Identificación de la tarjeta de taller	Card_Identification_____
	Fecha de caducidad de la tarjeta de taller	dd/mm/aaaa

19 ***El incidente y el fallo más recientes registrados en la VU***

	Identificador del bloque	----------!×🖷----------
	Hora y fecha del incidente más reciente	! dd/mm/aaaa hh:mm
	Hora y fecha del fallo más reciente	× dd/mm/aaaa hh:mm

20 ***Información sobre el control del exceso de velocidad***

	Identificador del bloque	----------▷▷----------
	Fecha y hora del último CONTROL DEL EXCESO DE VELOCIDAD	▷▯dd/mm/aaaa hh:mm
	Fecha/hora del primer exceso de velocidad y número de incidentes de exceso de velocidad desde	▷▷dd/mm/aaaa hh:mm (nnn)

21 ***Registro de excesos de velocidad***

21.1	Identificador de bloque «Primer exceso de velocidad después del último calibrado»	--------▷▷⍑---------
21.2	Identificador de bloque «Los 5 incidentes más graves ocurridos en los últimos 365 días»	-------▷▷(365)------
21.3	Identificador de bloque «El incidente más grave de cada uno de los últimos 10 días en que se hayan producido incidentes de este tipo»	-------▷▷(10)-------
21.4	Identificador de registro	----------
	Fecha, hora y duración	▷▷dd/mm/aaaa hh:mm hhhmm
	Velocidades máxima y media, n.º de incidentes similares este día	xxx km/h xxx km/h(xxx)
	Apellido(s) del conductor	⊙ Last_Name_____
	Nombre del conductor	First_Name_____
	Identificación de la tarjeta del conductor	Card_Identification_____
21.5	Si no existe registro de exceso de velocidad en un bloque	▷▷---

22 ***Información manuscrita***

	Identificador del bloque	----------
22.1	Lugar de control	▯• .....
22.2	Firma del controlador	▯ .....
22.3	Hora de comienzo	◷+ .....
22.4	Hora de conclusión	+◷ .....
22.5	Firma del conductor	⊙ .....

«Información manuscrita»; dejar suficientes líneas en blanco sobre el elemento manuscrito para poder escribir la información solicitada o firmar.

23 ***Las tarjetas más recientes introducidas en la VU***
Identificador del bloque
23.1 Tarjeta introducida
Identificador de registro
Tipo de tarjeta, Generación, Versión, Fabricante (*)
Identificación de la tarjeta
Número de serie de la tarjeta
Fecha y hora de la última inserción de la tarjeta

```
-------- ⊟■⊙ --------


----
⍑ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/aaaa hh:mm
```

(*) (todo en una sola línea)
con
tipo de tarjeta: Pictograma, un carácter + espacio
gen: GEN1 o GEN2, 4 caracteres + espacio
versión: Hasta 10 caracteres
MC: código del fabricante, 3 caracteres

3. ESPECIFICACIONES DE LOS DOCUMENTOS IMPRESOS

En este capítulo se han empleado las siguientes convenciones para la notación:

N	Imprimir bloque o registro número N
N	Imprimir bloque o registro número N, repetido tantas veces como sea necesario
X/Y	Imprimir bloques o registros X o Y según proceda, y repetidos tantas veces como sea necesario.

3.1. **Impresión diaria de las actividades del conductor almacenadas en la tarjeta**

PRT_008 La impresión diaria de las actividades del conductor almacenadas en la tarjeta deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del controlador (si se inserta una tarjeta de control en la VU)
3	Identificación del conductor (según la tarjeta cuyos datos se imprimen + GEN)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
5	Identificación de la VU (VU cuya impresión se obtiene + GEN)
6	Último calibrado de la VU actual
7	Último control pasado por el conductor sometido a la inspección
8	Delimitador de las actividades del conductor
8a	Condición «Fuera de ámbito» al comienzo de este día
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Actividades del conductor por orden de ocurrencia
11	Delimitador del resumen diario

11.4	Lugares introducidos en orden cronológico
11.5	Datos GNSS
11.6	Totalidad de actividades
12.1	Delimitador de incidentes o fallos almacenados en la tarjeta
12.4	Registro de incidentes/fallos (últimos 5 incidentes o fallos almacenados en la tarjeta)
13.1	Delimitador de incidentes o fallos almacenados en la VU
13.4	Registro de incidentes/fallos (últimos 5 incidentes o fallos almacenados o en curso en la VU)
22.1	Lugar de control
22.2	Firma del controlador
22.5	Firma del conductor

3.2. **Impresión diaria de las actividades del conductor almacenadas en la VU**

PRT_009 La impresión diaria de las actividades del conductor almacenadas en la VU deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del titular de la tarjeta (para todas las tarjetas insertadas en la VU + GEN)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
5	Identificación de la VU (VU cuya impresión se obtiene + GEN)
6	Último calibrado de esta VU
7	Último control realizado en este tacógrafo
9	Delimitador de las actividades del conductor
10	Delimitador de la ranura del conductor (ranura 1)
10a	Condición «Fuera de ámbito» al comienzo de este día
10.1 / 10.2 / 10.3 /10.3a / 10.4	Actividades en orden cronológico (ranura del conductor)
10	Delimitador de la ranura del segundo conductor (ranura 2)
10a	Condición «Fuera de ámbito» al comienzo de este día
10.1 / 10.2 / 10.3 /10.3a / 10.4	Actividades en orden cronológico (ranura del segundo conductor)
11	Delimitador del resumen diario
11.1	Síntesis de los intervalos sin tarjeta en la ranura del conductor
11.4	Lugares introducidos en orden cronológico
11.5	Datos GNSS
11.6	Totalidad de actividades
11.2	Resumen de los intervalos sin tarjeta en la ranura del segundo conductor
11.4	Lugares introducidos en orden cronológico
11.5	Datos GNSS

11.7	Totalidad de actividades
11.3	Resumen de actividades por el conductor, incluidas ambas ranuras
11.4	Lugares introducidos por este conductor en orden cronológico
11.5	Datos GNSS
11.8	Totalidad de actividades relativas al conductor actual
13.1	Delimitador de incidentes/fallos
12.4	Registro de incidentes/fallos (últimos 5 incidentes o fallos almacenados o en curso en la VU)
13.1	Lugar de control
22.2	Firma del controlador
22.3	Hora de comienzo (espacio reservado a un conductor sin una tarjeta para indicar qué períodos le atañen o corresponden)
22.4	Hora de finalización
22.5	Firma del conductor

3.3. **Impresión de incidentes y fallos almacenados en la tarjeta**

PRT_010 La impresión de incidentes y fallos almacenados en la tarjeta deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del controlador (si se inserta una tarjeta de control en la VU + GEN)
3	Identificación del conductor (según la tarjeta cuyos datos se imprimen)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
12.2	Delimitador de incidentes
12.4	Registros de incidentes (todos los incidentes almacenados en la tarjeta)
12.3	Delimitador de fallos
12.4	Registros de fallos (todos los fallos almacenados en la tarjeta)
22.1	Lugar de control
22.2	Firma del controlador
22.5	Firma del conductor

3.4. **Impresión de incidentes y fallos almacenados en la VU**

PRT_011 La impresión de incidentes y fallos almacenados en la VU deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del titular de la tarjeta (para todas las tarjetas insertadas en la VU + GEN)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)

13.2	Delimitador de incidentes
13.4	Registros de incidentes (todos los incidentes almacenados o en curso en la VU)
13.3	Delimitador de fallos
13.4	Registros de fallos (todos los fallos almacenados o en curso en la VU)
22.1	Lugar de control
22.2	Firma del controlador
22.5	Firma del conductor

3.5. **Impresión de datos técnicos**

PRT_012 La impresión de datos técnicos deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del titular de la tarjeta (para todas las tarjetas insertadas en la VU + GEN)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
14	Identificación de la VU
15	Identificación del sensor
15.1	Datos de emparejamiento del sensor (todos los datos existentes en orden cronológico)
16	Identificación de GNSS
16.1	Datos de acoplamiento del dispositivo GNSS externo (todos los datos existentes en orden cronológico)
17	Delimitador de los datos de calibrado
17.1	Registros de calibrado (todos los registros disponibles en orden cronológico)
18	Delimitador del ajuste de hora
18.1	Registros de ajuste de hora (todos los registros disponibles acerca del ajuste de hora y de los registros de los datos de calibrado)
19	El incidente y el fallo más recientes registrados en la VU

3.6. **Impresión de excesos de velocidad**

PRT_013 La impresión por exceso de velocidad deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificación del titular de la tarjeta (para todas las tarjetas insertadas en la VU + GEN)
4	Identificación del vehículo (vehículo del que se obtiene el documento impreso)
20	Información sobre el control del exceso de velocidad
21.1	Identificador de los datos sobre el exceso de velocidad
21.4/21.5	Primer exceso de velocidad después del último calibrado

21.2	Identificador de los datos sobre el exceso de velocidad
21.4/21.5	Los 5 incidentes más graves de exceso de velocidad ocurridos en los últimos 365 días
21.3	Identificador de los datos sobre el exceso de velocidad
21.4/21.5	El incidente más grave de exceso de velocidad en cada uno de los 10 últimos días en que hayan ocurrido incidentes de este tipo
22.1	Lugar de control
22.2	Firma del controlador
22.5	Firma del conductor

3.7. **Historial de tarjetas insertadas**

PRT_014 La impresión del historial de tarjetas insertadas deberá efectuarse con arreglo al formato siguiente:

1	Fecha y hora en la que se imprime el documento
2	Tipo de documento impreso
3	Identificaciones del titular de la tarjeta (para todas las tarjetas insertadas en la VU)
23	La tarjeta más reciente introducida en la VU
23.1	Las tarjetas introducidas (hasta 88 registros)
12.3	Delimitador de fallos

Apéndice 5

VISUALIZACIÓN

En este apéndice se utilizan las siguientes convenciones para la notación de formatos:

— los caracteres impresos **en negrita** indican texto legible en la visualización (la visualización aparece en caracteres normales),

— los caracteres normales indican variables (pictogramas o datos) que hay que sustituir por sus valores en la visualización:

  — dd mm aaaa: día, mes, año,

  — hh: horas,

  — mm: minutos,

  — D: pictograma de duración,

  — EF: combinación de pictogramas de incidente o fallo,

  — O: pictograma de modo de funcionamiento.

DIS_001 En la visualización, el aparato de control deberá utilizar los formatos siguientes:

Datos	Formato
Visualización por defecto	
Hora local	hh:mm
Modo de funcionamiento	O
Información relativa al conductor	1 Dhh**h**mm ▮▮hh**h**mm
Información relativa al segundo conductor	2 Dhh**h**mm
Condición fuera de ámbito abierta	OUT
Visualización de alerta	
Superación del tiempo de conducción continua	1 ☕ hh**h**mm ▮▮hh**h**mm
Incidente o fallo	EF
Otras visualizaciones	
Fecha UTC Hora	UTC dd/mm/aaaa o bien UTC dd/mm/aaaa hh:mm
Tiempo de conducción continua y tiempo de descanso acumulado del conductor	1 ☕ hh**h**mm ▮▮hh**h**mm
Tiempo de conducción continua y tiempo de descanso acumulado del segundo conductor	2 ☕ hh**h**mm ▮▮hh**h**mm
Tiempo de conducción acumulado del conductor durante la semana anterior y la actual	1 ☕ ▮▮ hhh**h**mm
Tiempo de conducción acumulado del segundo conductor durante la semana anterior y la actual	2 ☕ ▮▮ hhh**h**mm

Apéndice 6

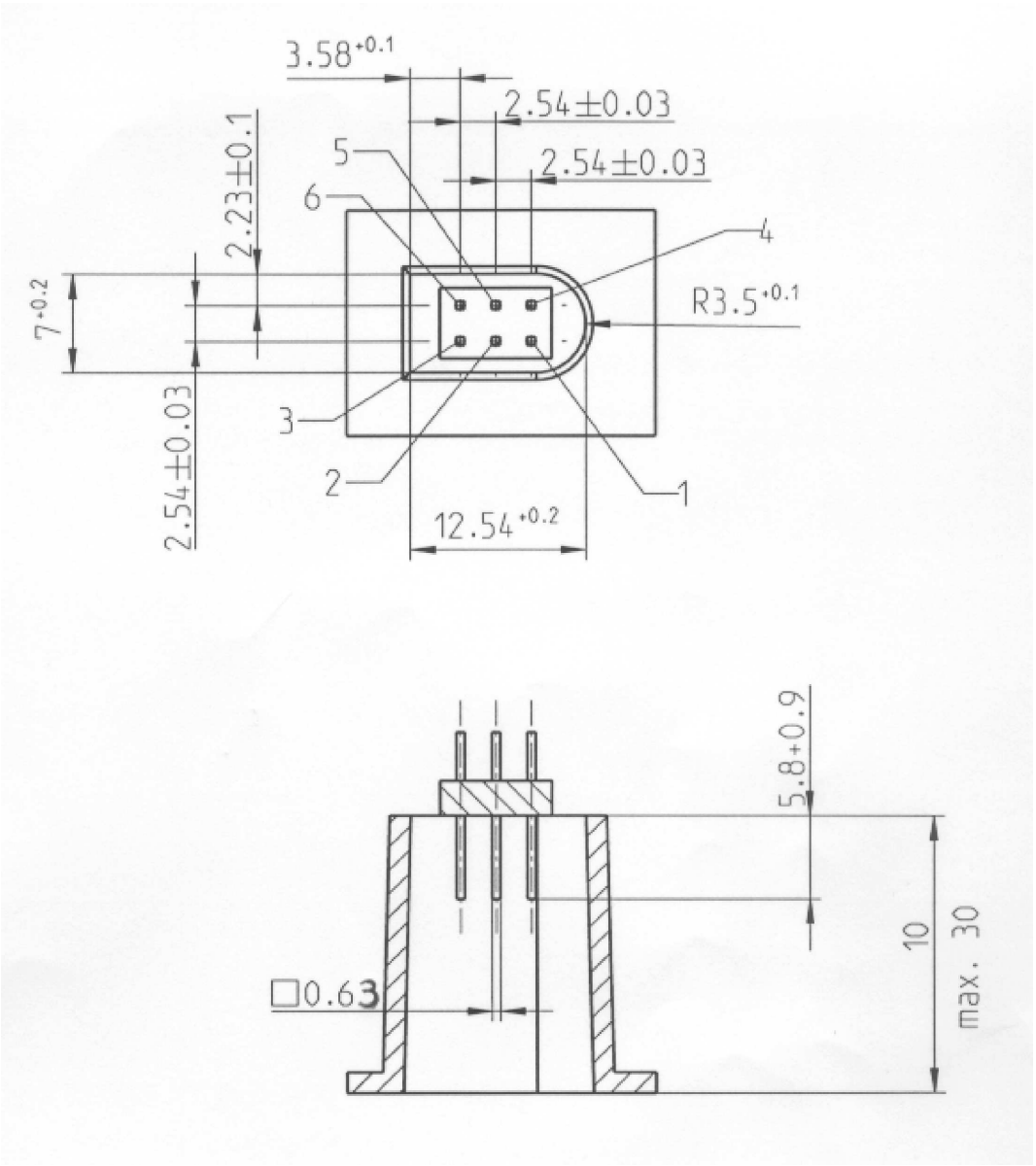
CONECTOR FRONTAL PARA EL CALIBRADO Y LA TRANSFERENCIA DE DATOS

ÍNDICE

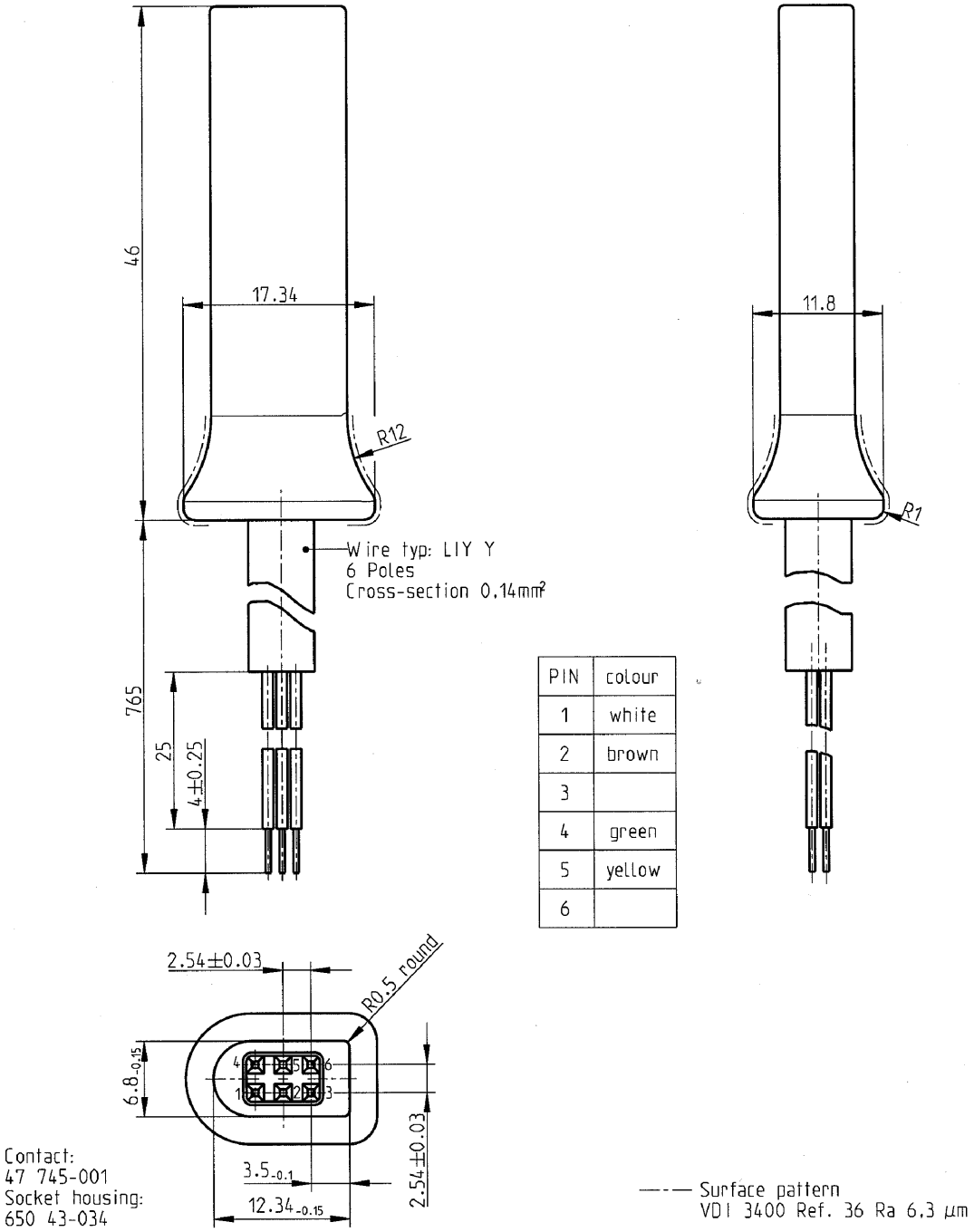
1. EQUIPO INFORMÁTICO

1.1. **Conector**

INT_001 El conector de transferencia/calibrado deberá tener 6 patillas y ser accesible en el panel frontal sin necesidad de desconectar ninguno de los elementos del tacógrafo, y sus dimensiones se ajustarán al siguiente esquema (dimensiones en milímetros):



La siguiente ilustración muestra una clavija de acoplamiento típica de 6 patillas:



1.2. **Asignación de contactos**

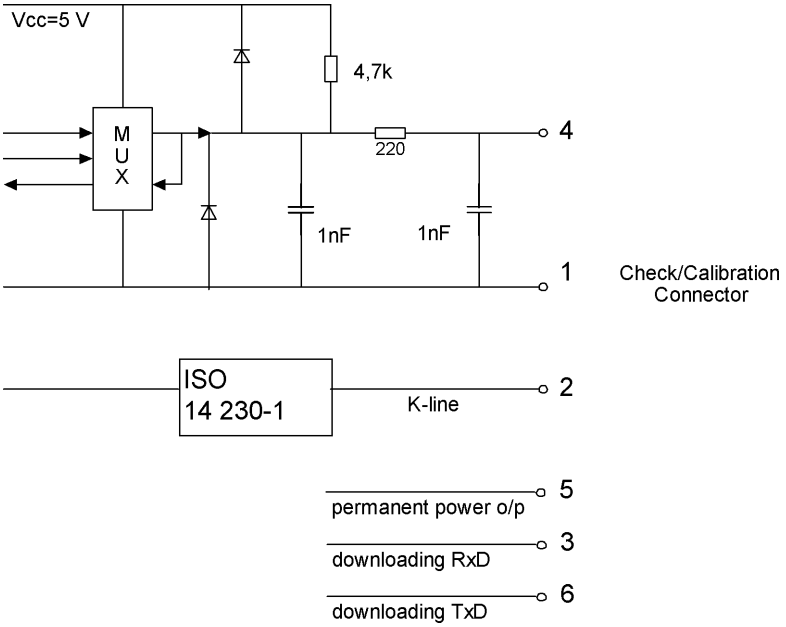
INT_002 Los contactos se asignarán de acuerdo con la tabla siguiente:

Patilla	Descripción	Observaciones
1	Polo negativo batería	Conectado al polo negativo de la batería del vehículo
2	Comunicación de datos	Línea K (ISO 14230-1)

Patilla	Descripción	Observaciones
3	Transferencia RxD	Entrada de datos en el tacógrafo
4	Señal de entrada/salida	Calibrado
5	Salida permanente de potencia	Se especifica que el intervalo de tensiones debe ser el de la potencia del vehículo menos 3 V para tener en cuenta la caída de tensión en los circuitos de protección. Salida 40 mA
6	Transferencia RxD	Salida de datos del tacógrafo

1.3. **Diagrama de conjunto**

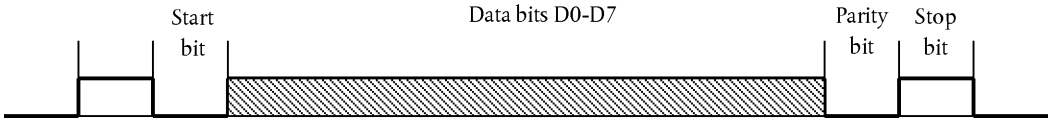
INT_003 El diagrama de conjunto será el siguiente:



2. INTERFAZ DE TRANSFERENCIA

INT_004 La interfaz de transferencia deberá cumplir las especificaciones RS232.

INT_005 La interfaz de transferencia deberá utilizar un bit de arranque, ocho bits de datos con el bit LSB primero, un bit de paridad par y un bit de parada.



Organización de los bytes de datos

Bit de arranque: un bit de nivel lógico 0;

Bits de datos: transmitidos con LSB primero;

Bit de paridad: paridad par

Bit de parada: un bit de nivel lógico 1

Cuando se transmitan datos numéricos compuestos de más de un byte, el byte más significativo se transmitirá el primero, y el byte menos significativo el último.

INT_006 La velocidad de transmisión deberá poder ajustarse entre 9 600 bps y 115 200 bps. La transmisión deberá efectuarse a la velocidad más alta posible; la velocidad inicial en baudios al comenzar la comunicación se fija en 9 600 bps.

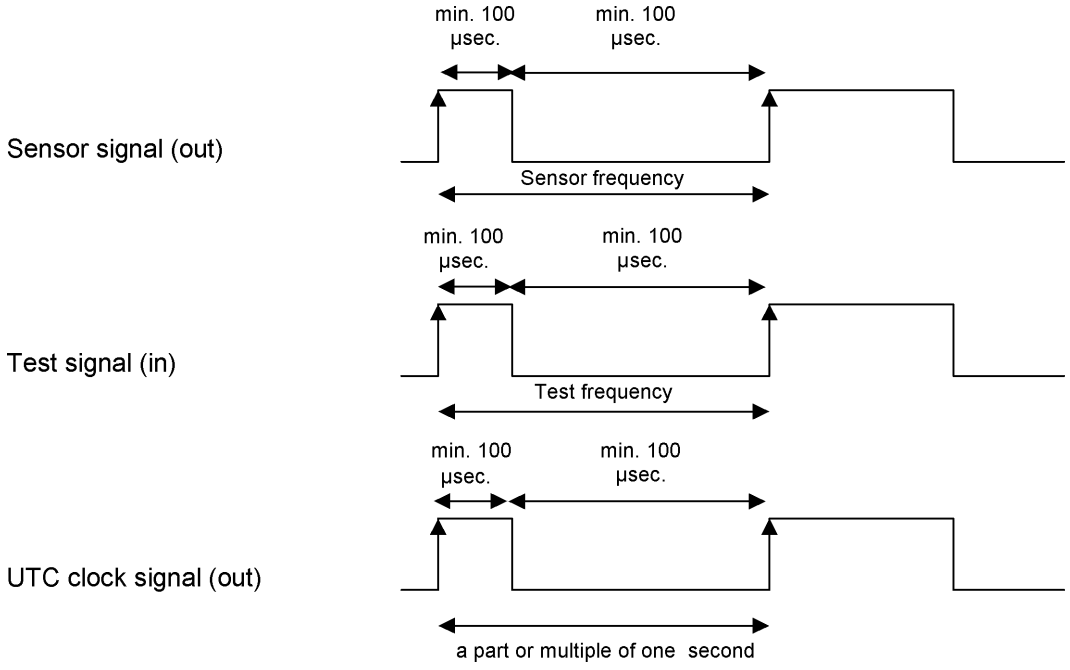
3. INTERFAZ DE CALIBRADO

INT_007 La comunicación de datos deberá cumplir lo dispuesto en la norma ISO 14230-1 Vehículos de carretera — Sistemas de diagnóstico — Protocolo Keyword 2000 — Parte 1: Nivel físico, Primera edición: 1999.

INT_008 La señal de entrada/salida deberá cumplir las siguientes especificaciones eléctricas:

Parámetro	Mínimo	Típico	Máximo	Observaciones
U_{low} (in)			1,0 V	I = 750 µA
U_{high} (in)	4 V			I = 200 µA
Frecuencia			4 kHz	
U_{low} (out)			1,0 V	I = 1 mA
U_{high} (out)	4 V			I = 1 mA

INT_009 La señal de entrada/salida deberá cumplir los siguientes diagramas de relaciones de tiempo:



Apéndice 7

PROTOCOLOS DE TRANSFERENCIA DE DATOS

ÍNDICE

1. INTRODUCCIÓN

En el presente apéndice se especifican los procedimientos que se deben utilizar para llevar a cabo los diferentes tipos de transferencia de datos a un medio de almacenamiento externo (ESM), así como los protocolos que es preciso aplicar para garantizar la corrección de dichas transferencias y la total compatibilidad del formato de los datos transferidos, a fin de que un controlador cualquiera pueda inspeccionar dichos datos y comprobar su autenticidad e integridad antes de analizarlos.

1.1. Ámbito de aplicación

Se pueden transferir datos a un ESM:

— desde una unidad instalada en el vehículo (VU), mediante un equipo dedicado inteligente (IDE) conectado a la VU;

— desde una tarjeta de tacógrafo, mediante un IDE que incorpore un dispositivo de interfaz de tarjeta (IFD); y

— desde una tarjeta de tacógrafo y a través de una unidad instalada en el vehículo, mediante un IDE conectado a la VU.

Para poder verificar la autenticidad y la integridad de los datos transferidos que se encuentran almacenados en un ESM, dichos datos se transfieren con una firma añadida según lo dispuesto en el apéndice 11 (Mecanismos de seguridad comunes). También se transfieren la identificación del equipo de origen (VU o tarjeta) y sus certificados de seguridad (Estado miembro y equipamiento). La persona encargada de verificar los datos debe estar en posesión de una clave pública europea de confianza.

DDP_001 Los datos transferidos durante una sesión de transferencia deben almacenarse en el ESM en un solo archivo.

1.2. Acrónimos y notaciones

En el presente apéndice se utilizan los siguientes acrónimos:

AID Identificador de aplicación

ATR Respuesta a reinicio

CS Byte de la suma de control

DF Archivo dedicado

DS Sesión de diagnóstico

EF Archivo elemental

ESM Medio de almacenamiento externo

FID Identificador de archivo (ID de archivo)

FMT Byte de formato (primer byte de la cabecera del mensaje)

ICC Tarjeta de circuito integrado

IDE Equipo dedicado inteligente: equipo empleado para realizar la transferencia de datos al ESM (por ejemplo un ordenador personal)

IFD Dispositivo de interfaz

KWP Protocolo Keyword 2000

LEN Byte de longitud (el último byte de la cabecera del mensaje)

PPS Selección de los parámetros de protocolo

PSO Realizar operación de seguridad

SID Identificador de servicio

SRC Byte de origen

TGT Byte de destino

TLV Valor de longitud de la etiqueta

TREP Parámetro de la respuesta a la petición de transferencia

TRTP Parámetro de la petición de transferencia

VU Unidad instalada en el vehículo

2. TRANSFERENCIA DE LOS DATOS DE LA VU

2.1. **Procedimiento de transferencia**

A fin de realizar una transferencia de los datos de la VU, el operario debe efectuar las siguientes operaciones:

— introducir su tarjeta de tacógrafo en una ranura de la VU (*);

— conectar el IDE al conector de transferencia de la VU;

— establecer una conexión entre el IDE y la VU;

— seleccionar en el IDE los datos que se van a transferir y enviar la petición a la VU; y

— cerrar la sesión de transferencia.

2.2. **Protocolo de transferencia de datos**

El protocolo presenta una estructura maestro-esclavo, de modo que el IDE actúa como maestro y la VU como esclavo.

La estructura, los tipos y el flujo de los mensajes se basan principalmente en el protocolo Keyword 2000 (KWP) (ISO 14230-2: Vehículos de carretera — Sistemas de diagnóstico — Protocolo Keyword 2000 — Parte 2: Nivel de enlace de datos).

El nivel de aplicación se basa principalmente en el proyecto actual de la norma ISO 14229-1 (Vehículos de carretera — Sistemas de diagnóstico — Parte 1: Servicios de diagnóstico, versión 6 de 22 de febrero de 2001).

2.2.1 *Estructura del mensaje*

DDP_002 El formato de todos los mensajes que intercambian el IDE y la VU presenta una estructura de tres partes:

— una cabecera compuesta por un byte de formato (FMT), un byte de destino (TGT), un byte de origen (SRC) y posiblemente un byte de longitud (LEN);

— un campo de datos compuesto por un byte identificador de servicio (SId) y un número variable de bytes de datos, que puede incluir un byte opcional de sesión de diagnóstico (DS_) o un byte opcional de parámetro de transferencia (TRTP o TREP); y

— una suma de control consistente en un byte de suma de control (CS).

Cabecera				Campo de datos					Suma de control
FMT	TGT	SRC	LEN	SId	DAT-OS	…	…	…	CS
4 bytes				Máx. 255 bytes					1 byte

(*) La tarjeta introducida activará los correspondientes derechos de acceso a la función de transferencia y a los datos. No obstante, se podrán transferir los datos almacenados en una tarjeta de conductor introducida en una de las ranuras de la VU siempre que no haya otro tipo de tarjeta en la otra ranura.

Los bytes TGT y SRC representan la dirección física del destinatario y del emisor del mensaje. Los valores son F0 Hex para el IDE y EE Hex para la VU.

El byte LEN es la longitud de la parte correspondiente al campo de datos.

El byte de suma de control es la suma de todos los bytes del mensaje tomados de 8 bits en 8 bits, en módulo 256, excluido el propio CS.

Los bytes FMT, SId, DS, TRTP y TREP se definen más adelante en este mismo documento.

DDP_003 Cuando la longitud de los datos que deba incluir el mensaje es mayor que el espacio disponible en la parte correspondiente al campo de datos, el mensaje se envía dividido en varios submensajes. Cada submensaje incorpora una cabecera, los mismos SId y TREP y un contador de dos bytes que indica el número de submensaje dentro del mensaje total. Al objeto de permitir la verificación de errores y la cancelación, el IDE confirma cada uno de los submensajes. El IDE puede aceptar el submensaje, solicitar su retransmisión, pedir a la VU que comience de nuevo o cancelar la transmisión.

DDP_004 Si el último submensaje contiene exactamente 255 bytes en el campo de datos, habrá que añadir un submensaje final con un campo de datos vacío (exceptuando los identificadores SId y TREP y el contador de submensaje) para indicar el final del mensaje.

Ejemplo:

Cabecera	SId	TREP	Mensaje	CS
4 bytes	Más de 255 bytes			

Se transmitirá como:

Cabecera	SId	TREP	00	01	Submensaje 1	CS
4 bytes	255 bytes					

Cabecera	SId	TREP	00	02	Submensaje 2	CS
4 bytes	255 bytes					

…

Cabecera	SId	TREP	xx	yy	Submensaje n	CS
4 bytes	Menos de 255 bytes					

o bien como:

Cabecera	SId	TREP	00	01	Submensaje 1	CS
4 bytes	255 bytes					

Cabecera	SId	TREP	00	02	Submensaje 2	CS
4 bytes	255 bytes					

…

Cabecera	SId	TREP	xx	yy	Submensaje n	CS
4 bytes	255 bytes					

Cabecera	SId	TREP	xx	yy + 1	CS
4 bytes	4 bytes				

2.2.2 *Tipos de mensajes*

El protocolo de comunicación para la transferencia de datos entre la VU y el IDE exige el intercambio de ocho tipos de mensajes diferentes.

La siguiente tabla resume dichos mensajes.

Estructura del mensaje	Máx. 4 bytes Cabecera				Máx. 255 bytes Datos			1 byte Suma de control
IDE -> <- VU	FMT	TGT	SRC	LEN	SId	DS_/TRTP	DATOS	CS
Petición de inicio de comunicación	81	EE	F0		81			E0
Respuesta positiva a la petición de inicio de comunicación	80	F0	EE	03	C1		EA, 8F	9B
Petición de inicio de la sesión de diagnóstico	80	EE	F0	02	10	81		F1
Respuesta positiva a la petición de inicio de diagnóstico	80	F0	EE	02	50	81		31
Servicio de control del enlace								
Verificar la velocidad en baudios (fase 1)								
9 600 Bd	80	EE	F0	04	87		01,01, 01	EC
19 200 Bd	80	EE	F0	04	87		01,01, 02	ED
38 400 Bd	80	EE	F0	04	87		01,01, 03	EE
57 600 Bd	80	EE	F0	04	87		01,01, 04	EF
115 200 Bd	80	EE	F0	04	87		01,01, 05	F0
Respuesta positiva a la petición de verificar la velocidad en baudios	80	F0	EE	02	C7		01	28
Velocidad de baudios de transición (fase 2)	80	EE	F0	03	87		02,03	ED
Envío de petición	80	EE	F0	0A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Respuesta positiva al envío de petición	80	F0	EE	03	75		00,FF	D5

Estructura del mensaje	Máx. 4 bytes Cabecera				Máx. 255 bytes Datos			1 byte Suma de control
IDE -> <- VU	FMT	TGT	SRC	LEN	SId	DS_/TRTP	DATOS	CS
Petición de transferencia de datos								
Visión general	80	EE	F0	02	36	01		97
Actividades	80	EE	F0	06	36	02	Fecha	CS
Incidentes y fallos	80	EE	F0	02	36	03		99
Datos pormenorizados sobre la velocidad	80	EE	F0	02	36	04		9A
Datos técnicos	80	EE	F0	02	36	05		9B
Transferencia de los datos de la tarjeta	80	EE	F0	02	36	06	Ranura	CS
Respuesta positiva a la petición de transferencia de datos	80	F0	EE	Len	76	TREP	Datos	CS
Petición de salida de la transferencia	80	EE	F0	01	37			96
Respuesta positiva a la petición de salida de la transferencia	80	F0	EE	01	77			D6
Petición de interrupción de la comunicación	80	EE	F0	01	82			E1
Respuesta positiva a la petición de interrupción de la comunicación	80	F0	EE	01	C2			21
Confirmación de submensaje	80	EE	F0	Len	83		Datos	CS
Respuestas negativas								
Denegación general	80	F0	EE	03	7F	SId pet.	10	CS
Servicio no admitido	80	F0	EE	03	7F	SId pet.	11	CS
Subfunción no admitida	80	F0	EE	03	7F	SId pet.	12	CS
Longitud del mensaje incorrecta	80	F0	EE	03	7F	Sid pet.	13	CS
Condiciones incorrectas o error en la secuencia de la petición	80	F0	EE	03	7F	SId pet.	22	CS
Petición no admisible	80	F0	EE	03	7F	SId pet.	31	CS
Envío no aceptado	80	F0	EE	03	7F	SId pet.	50	CS
Falta respuesta	80	F0	EE	03	7F	SId pet.	78	CS
Datos no disponibles	80	F0	EE	03	7F	SId pet.	FA	CS

Notas:

— SId pet. = el SId de la petición correspondiente.

— TREP = el TRTP de la petición correspondiente.

— Las casillas en negro significan que no se transmite ningún dato.

— El término envío (entendido desde el IDE) se utiliza para compatibilidad con la norma ISO 14229. Significa lo mismo que transferencia (entendida desde la VU).

— Los posibles contadores de submensaje de dos bytes no aparecen en la tabla.

— El valor «ranura» se corresponde con el número de la ranura, que puede ser 1 (tarjeta de la ranura del conductor) o 2 (tarjeta de la ranura del copiloto).

— En caso de que no se especifique la ranura, la VU seleccionará la ranura 1 si la tarjeta se inserta en esta ranura y solamente seleccionará 2 si así lo selecciona específicamente el usuario.

2.2.2.1 Start Communication Request (petición de inicio de comunicación) (SId 81)

DDP_005 El IDE envía este mensaje para establecer el enlace de comunicación con la VU. Las comunicaciones iniciales se hacen siempre a 9 600 baudios (hasta que la velocidad en baudios se cambia utilizando los servicios adecuados de control del enlace).

2.2.2.2 Positive Response Start Communication (respuesta positiva a la petición de inicio de comunicación) (SId C1)

DDP_006 La VU envía este mensaje para responder positivamente a una petición de inicio de comunicación. Incluye los dos bytes de clave EA y 8F, indicativos de que la unidad admite un protocolo con una cabecera que incluya información sobre el destino, el origen y la longitud del mensaje.

2.2.2.3 Start Diagnostic Session Request (petición de inicio de la sesión de diagnóstico) (SId 10)

DDP_007 El IDE envía el mensaje de petición de inicio de la sesión de diagnóstico para solicitar una nueva sesión de diagnóstico con la VU. La subfunción «sesión por defecto» (*default session*) (81 Hex) indica que va a abrirse una sesión de diagnóstico estándar.

2.2.2.4 Positive Response Start Diagnostic (respuesta positiva a la petición de inicio de diagnóstico) (SId 50)

DDP_008 La VU envía el mensaje de respuesta positiva a la petición de inicio de diagnóstico para responder positivamente a la solicitud de sesión de diagnóstico.

2.2.2.5 Link Control Service (servicio de control del enlace) (SId 87)

DDP_052 El IDE utiliza el servicio de control del enlace para iniciar un cambio en la velocidad en baudios. Este cambio se lleva a cabo en dos etapas. En la primera, el IDE propone el cambio en la velocidad en baudios, indicando la nueva velocidad. Al recibir un mensaje positivo de la VU, el IDE envía a la VU una confirmación del cambio en la velocidad en baudios (etapa 2). A continuación, el IDE cambia a la nueva velocidad en baudios. Tras recibir la confirmación la VU, cambia a la nueva velocidad en baudios.

2.2.2.6 Link Control Positive Response (respuesta positiva al control del enlace) (SId C7)

DDP_053 La VU envía la respuesta positiva al control del enlace para contestar positivamente a la petición de servicio del control del enlace (etapa 1). Téngase en cuenta que no se da respuesta a la solicitud de confirmación (etapa 2).

2.2.2.7 Request Upload (envío de petición) (SId 35)

DDP_009 El IDE emite el mensaje de envío de petición para especificar a la VU que se solicita una operación de transferencia. Para cumplir los requisitos de la norma ISO 14229, se incluyen entre los datos la dirección, el tamaño y el formato de los datos solicitados. Dado que el IDE no los conoce antes de la transferencia, la dirección de la memoria se configura a 0, el formato está descifrado y descomprimido y el tamaño de la memoria se fija en el máximo.

2.2.2.8 Positive Response Request Upload (respuesta positiva al envío de petición) (SId 75)

DDP_010 La VU envía el mensaje de respuesta positiva al envío de petición para indicar al IDE que la VU está preparada para transferir datos. Para cumplir los requisitos de la norma ISO 14229, en este mensaje de respuesta positiva se incluyen datos, indicando al IDE que los ulteriores mensajes de respuesta positiva a la transferencia de datos incluirán un máximo de 00FF hex bytes.

2.2.2.9 Transfer Data Request (petición de transferencia de datos) (SId 36)

DDP_011 El IDE envía la petición de transferencia de datos para especificar a la VU el tipo de datos que se van a transferir. Un parámetro de petición de transferencia (TRTP) de un byte indica el tipo de transferencia.

Existen seis tipos de transferencias de datos:

— resumen (TRTP 01);

— actividades de una fecha específica (TRTP 02);

— incidentes y fallos (TRTP 03);

— datos pormenorizados sobre la velocidad (TRTP 04);

— datos técnicos (TRTP 05); y

— transferencia de datos de la tarjeta (TRTP 06).

DDP_054 Es obligatorio que el IDE solicite la transferencia de datos resumen (TRTP 01) durante una sesión de transferencia, ya que solo así se asegura que los certificados de la VU se registran en el archivo transferido (y se permite la verificación de la firma digital).

En el segundo caso (TRTP 02), el mensaje de petición de transferencia de datos incluye la indicación del día natural (en formato `TimeReal`) cuyos datos se van a transferir.

2.2.2.10 Positive Response Transfer Data (respuesta positiva a la petición de transferencia de datos) (SId 76)

DDP_012 La VU envía la respuesta positiva a la petición de transferencia de datos como contestación a la petición de transferencia de datos. Este mensaje contiene los datos solicitados, junto con un parámetro de respuesta a la solicitud de transferencia (TREP) correspondiente al TRTP de la petición.

DDP055 En el primer caso (TREP 01), la VU envía datos que ayudan al operario del IDE a seleccionar los datos que quiere transferir. La información contenida en este mensaje es la siguiente:

— certificados de seguridad;

— identificación del vehículo;

— fecha y hora actuales de la VU;

— fecha máxima y mínima transferible (datos de la VU);

— indicación de presencia de tarjetas en la VU;

— transferencia previa a una empresa;

— bloqueos introducidos por empresas; e

— inspecciones anteriores.

2.2.2.11 Request Transfer Exit (petición de salida de la transferencia) (SId 37)

DDP_013 El IDE envía el mensaje de petición de salida de la transferencia para informar a la VU de que la sesión de transferencia ha terminado.

2.2.2.12 Positive Response Request Transfer Exit (respuesta positiva a la petición de salida de la transferencia) (SId 77)

DDP_014 La VU envía el mensaje de respuesta positiva a la petición de salida de la transferencia para confirmar la petición de salida de la transferencia.

2.2.2.13 Stop Communication Request (petición de interrupción de la comunicación) (SId 82)

DDP_015 El IDE envía el mensaje de petición de interrupción de la comunicación para desconectar el enlace de comunicación con la VU.

2.2.2.14 Positive Response Stop Communication (respuesta positiva a la petición de interrupción de la comunicación) (SId C2)

DDP_016 La VU envía el mensaje de respuesta positiva a la petición de interrupción de la comunicación para confirmar la petición de interrupción de la comunicación.

2.2.2.15 Acknowledge Sub Message (confirmación de submensaje) (SId 83)

DDP_017 El IDE envía el mensaje de confirmación de submensaje para confirmar la recepción de cada una de las partes de un mensaje que se transmiten como diversos submensajes. El campo de datos contiene el SId recibido de la VU y un código de dos bytes que se interpreta de la manera siguiente:

— MsgC +1 confirma la correcta recepción del submensaje número MsgC.

El IDE solicita a la VU que envíe el siguiente submensaje.

— MsgC indica un problema en la recepción del submensaje número MsgC.

El IDE solicita a la VU que vuelva a enviar el submensaje.

— FFFF solicita la terminación del mensaje.

El IDE puede utilizar este código para terminar la transmisión del mensaje de la VU por el motivo que fuera.

El último submensaje de un mensaje (byte LEN < 255) se puede confirmar con cualquiera de estos códigos, o bien puede dejarse sin confirmar.

Respuestas de la VU que se componen de varios submensajes:

— Positive Response Transfer Data (respuesta positiva a la petición de transferencia de datos) (SId 76)

2.2.2.16 Negative Response (respuesta negativa) (SId 7F)

DDP_018 La VU envía el mensaje de respuesta negativa como contestación a los mensajes de petición anteriores cuando no puede satisfacer la petición de que se trate. Los campos de datos del mensaje incluyen el SId de la respuesta (7F), el SId de la petición y un código que especifica el motivo de la respuesta negativa. Están disponibles los códigos siguientes:

— 10: rechazo general

La acción solicitada no se puede llevar a cabo por un motivo distinto de los enumerados a continuación.

— 11: servicio no admitido

No se entiende el SId de la petición.

— 12: subfunción no admitida

No se entiende el DS_ o el TRTP de la petición, o bien no hay más submensajes que transmitir.

— 13: longitud del mensaje incorrecta

La longitud del mensaje es incorrecta.

— 22: condiciones incorrectas o error en la secuencia de la petición

El servicio requerido no está activo o la secuencia de mensajes de petición es incorrecta.

— 31: solicitud no admisible

El registro del parámetro de la solicitud (campo de datos) no es válido.

— 50: envío no aceptado

No se puede llevar a cabo la petición (la VU se encuentra en un modo de funcionamiento inadecuado o tiene un fallo interno).

— 78: falta respuesta

La acción solicitada no se puede llevar a cabo a tiempo y la VU no está preparada para aceptar otra petición.

— FA: datos no disponibles

El objeto de datos de una petición de transferencia de datos no está disponible en la VU (por ejemplo, no se ha introducido una tarjeta, etc.).

2.2.3 *Flujo del mensaje*

A continuación se describe el flujo normal de un mensaje durante un procedimiento normal de transferencia de datos:

IDE		VU
Petición de inicio de comunicación	⇨ ⇦	Respuesta positiva
Petición de inicio del servicio de diagnóstico	⇨ ⇦	Respuesta positiva
Envío de petición	⇨ ⇦	Respuesta positiva

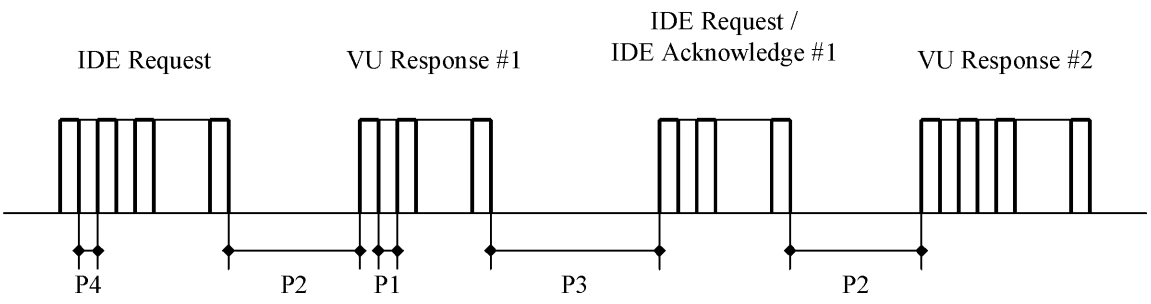
IDE		VU
Resumen de peticiones de transferencia de datos	⇨	
	⇦	Respuesta positiva
Petición de transferencia de datos nº 2	⇨	
	⇦	Respuesta positiva nº 1
Confirmación de submensaje nº 1	⇨	
	⇦	Respuesta positiva nº 2
Confirmación de submensaje nº 2	⇨	
	⇦	Respuesta positiva nº m
Confirmación de submensaje nº m	⇨	
	⇦	Respuesta positiva (Campo de datos < 255 bytes)
Confirmación de submensaje (opcional)	⇨	
…		
Petición de transferencia de datos nº n	⇨	
	⇦	Respuesta positiva
Petición de salida de la transferencia	⇨	
	⇦	Respuesta positiva
Petición de interrupción de la comunicación	⇨	
	⇦	Respuesta positiva

2.2.4 *Sincronización*

DDP_019 Los parámetros de sincronización que aparecen en el gráfico siguiente son importantes durante el funcionamiento normal:

Gráfico 1

Flujo del mensaje, sincronización



Donde:

P1 = tiempo entre dos bytes en la respuesta de la VU.

P2 = tiempo transcurrido desde el final de la petición del IDE hasta el comienzo de la respuesta de la VU, o desde el final de la confirmación del IDE hasta el comienzo de la siguiente respuesta de la VU.

P3 = tiempo transcurrido desde el final de la respuesta de la VU hasta el comienzo de una nueva petición del IDE, o desde el final de la respuesta de la VU hasta el principio de la confirmación del IDE, o desde el final de la petición del IDE hasta el comienzo de una nueva petición del IDE si la VU no responde.

P4 = tiempo entre dos bytes en la petición del IDE.

P5 = valor ampliado de P3 para la transferencia de los datos de la tarjeta.

La siguiente tabla muestra los valores admisibles para los parámetros de sincronización (conjunto de parámetros de sincronización ampliados KWP, empleado en caso de direccionamiento físico para lograr una comunicación más rápida).

Sincronización Parámetro	Límite inferior Valor (ms)	Límite superior Valor (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minutos

(*) Si la VU envía una respuesta negativa con un código que signifique «petición recibida correctamente, pendiente de respuesta», este valor se amplía hasta el mismo valor límite máximo de P3.

2.2.5 *Gestión de errores*

Si se produce un error durante el intercambio de mensajes, el esquema de flujo del mensaje se modifica en función de qué equipo haya detectado el error y de qué mensaje haya generado el error.

Los gráficos 2 y 3 muestran los procedimientos de gestión de errores de la VU y del IDE, respectivamente.

2.2.5.1 Fase de inicio de la comunicación

DDP_020 Si el IDE detecta un error durante la fase de inicio de la comunicación, ya sea debido a la sincronización o a la corriente de bits, esperará durante un período P3 mín. antes de enviar de nuevo la petición.

DDP_021 Si la VU detecta un error en la secuencia procedente del IDE, no enviará respuesta y esperará durante un período P3 máx. para recibir otro mensaje de petición de inicio de comunicación.

2.2.5.2 Fase de comunicación

Se pueden definir dos zonas distintas de gestión de errores:

1. **La VU detecta un error en la transmisión del IDE**

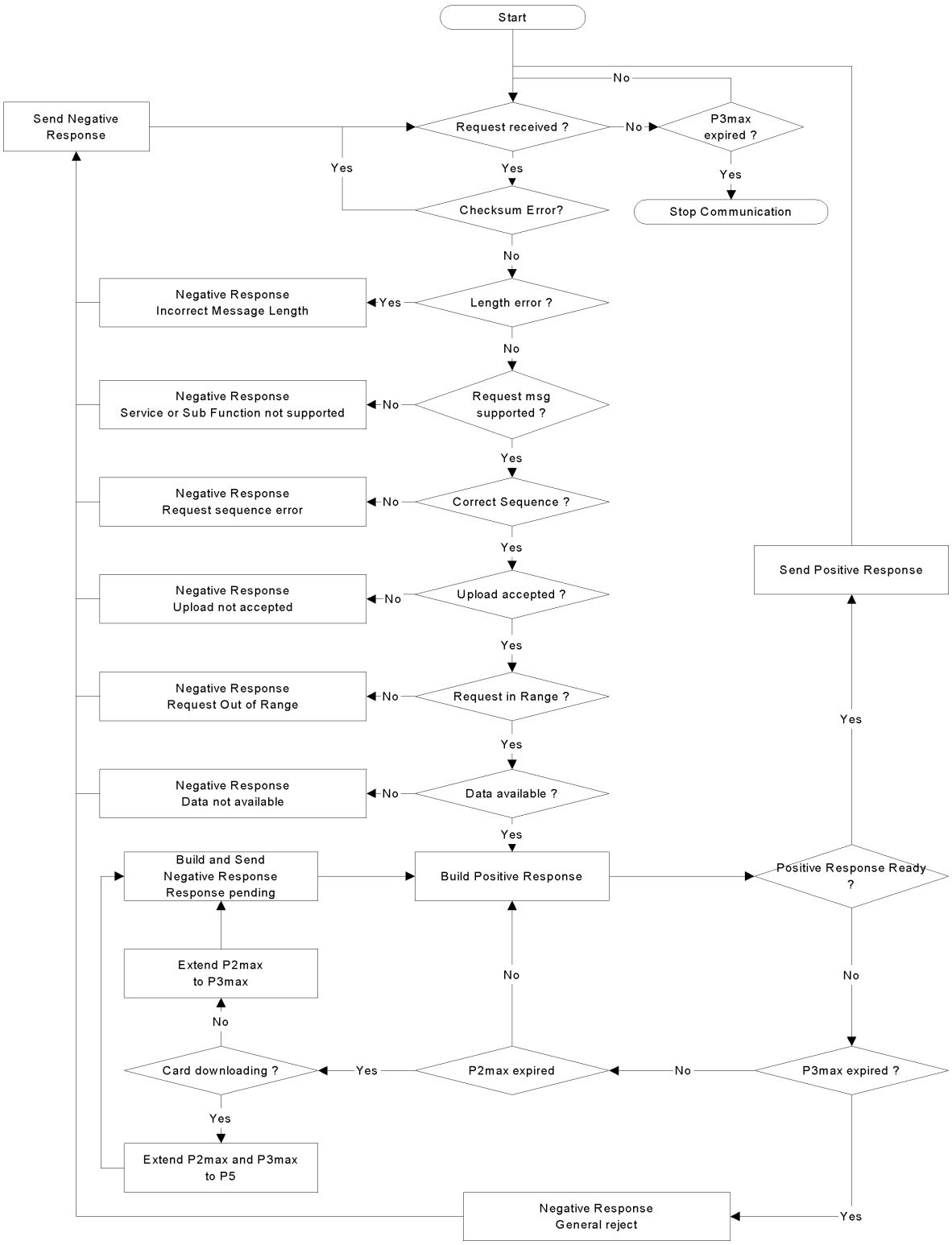
DDP_022 Para cada mensaje que reciba, la VU buscará errores de sincronización, errores de formato de byte (por ejemplo, violaciones de los bits de inicio y de paro) y errores de trama (número de bytes recibidos incorrecto, byte de la suma de control incorrecto).

DDP_023 Si la VU detecta uno de los errores anteriores, no envía respuesta ni hace caso del mensaje recibido.

DDP_024 La VU puede detectar otros errores en el formato o en el contenido del mensaje recibido (por ejemplo, tipo de mensaje inadmisible), aunque el mensaje cumpla los requisitos en cuanto a longitud y suma de control. En tal caso, la VU deberá contestar al IDE con un mensaje de respuesta negativa que especifique la naturaleza del error. (NOTA: el siguiente organigrama no debe traducirse, ni tampoco los que figuran en las próximas páginas).

Gráfico 2

Gestión de errores de la VU



2. **EL IDE DETECTA UN ERROR EN LA TRANSMISIÓN DE LA VU**

DDP_025 Para cada mensaje que reciba, el IDE buscará errores de sincronización, errores de formato de byte (por ejemplo, violaciones de los bits de inicio y de paro) y errores de trama (número de bytes recibidos incorrecto, byte de la suma de control incorrecto).

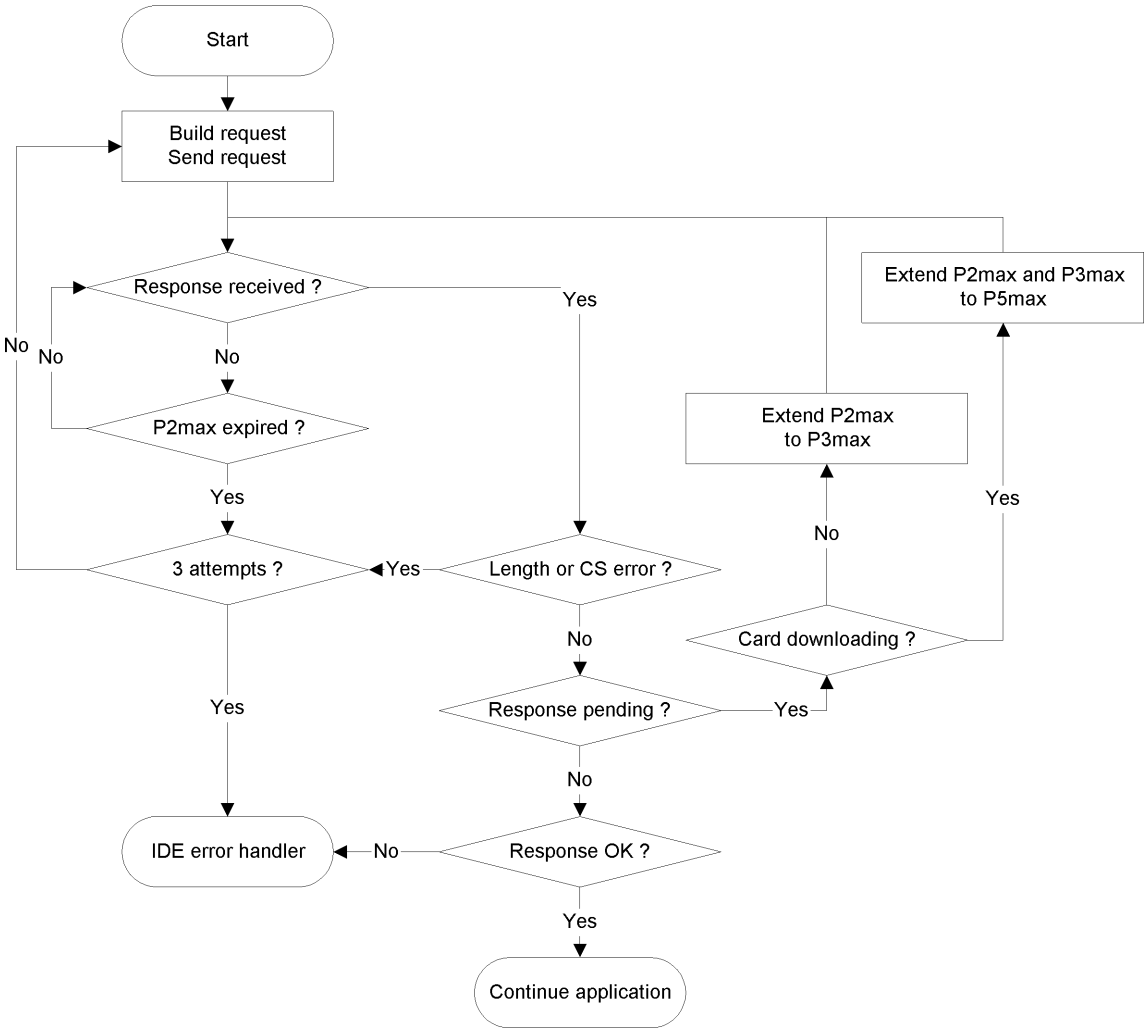
DDP_026 El IDE deberá detectar errores de secuencia; es decir, errores en los incrementos del contador de submensajes en mensajes sucesivos.

DDP_027 Si el IDE detecta un error o transcurre el período P2máx. sin que se haya recibido contestación de la VU, el mensaje de petición se envía de nuevo hasta un máximo de tres transmisiones en total. A efectos de esta detección de errores, una confirmación de submensaje se considerará como petición a la VU.

DDP_028 El IDE deberá esperar durante al menos un período P3mín. antes de comenzar cada transmisión; el período de espera se medirá a partir del momento de ocurrencia del último bit de paro calculado después de haberse detectado el error.

Gráfico 3

Gestión de errores del IDE



2.2.6 *Contenido del mensaje de respuesta*

En este apartado se especifica el contenido de los campos de datos incluidos en los diferentes mensajes de respuesta positiva.

Los elementos de datos se definen en el apéndice 1 (Diccionario de datos).

Observaciones: En el caso de las transferencias de segunda generación, cada elemento de datos de primer nivel está representado por un conjunto de registros, incluso si solo contiene un registro. Los conjuntos de registros empiezan con una cabecera, que contiene el tipo de registro, el tamaño del registro y el número de registros. En las tablas recogidas a continuación se denomina a los conjuntos de registros como «… RecordArray» (con cabecera).

2.2.6.1 Respuesta positiva a la petición de transferencia de datos «resumen»

DDP_029 El campo de datos del mensaje Positive Response Transfer Data Overview (respuesta positiva a la petición de transferencia de datos resumen) contiene los datos siguientes en este orden, con el SId 76 Hex, el TREP 01 Hex y el método adecuado de división y recuento de submensajes:

Estructura de datos de primera generación

Elemento de dato	Observaciones
MemberStateCertificate VUCertificate	Certificados de seguridad de la VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Identificación del vehículo
CurrentDateTime	Fecha y hora actuales de la VU
VuDownloadablePeriod	Período transferible
CardSlotsStatus	Tipo de tarjetas insertadas en la VU
VuDownloadActivityData	Última transferencia de la VU
VuCompanyLocksData	Todos los bloqueos introducidos por empresas almacenados. Si esta sección está vacía, únicamente se envía el mensaje «noOfLocks=0».
VuControlActivityData	Todos los registros de control almacenados en la VU. Si esta sección está vacía, únicamente se envía el mensaje «noOfControls=0».
Signature	Firma RSA de todos los datos (excepto los certificados) desde VehicleIdentificationNumber hasta el último byte del último VuControlActivityData.

Estructura de datos de segunda generación

Elemento de dato	Observaciones
MemberStateCertificateRecordArray	Certificado del Estado miembro
VUCertificateRecordArray	Certificado de la VU
VehicleIdentificationNumberRecordArray	Identificación del vehículo
VehicleRegistrationNumberRecordArray	Matrícula del vehículo
CurrentDateTimeRecordArray	Fecha y hora actuales de la VU
VuDownloadablePeriodRecordArray	Período transferible
CardSlotsStatusRecordArray	Tipo de tarjetas insertadas en la VU
VuDownloadActivityDataRecordArray	Última transferencia de la VU
VuCompanyLocksRecordArray	Todos los bloqueos introducidos por empresas almacenados. Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
VuControlActivityRecordArray	Todos los registros de control almacenados en la VU. Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
SignatureRecordArray	La firma ECC de todos los datos anteriores, excepto los certificados.

2.2.6.2 Respuesta positiva a la petición de transferencia de datos sobre actividades

DDP_030 El campo de datos del mensaje Positive Response Transfer Data Activities (respuesta positiva a la petición de transferencia de datos sobre actividades) contiene los datos siguientes en este orden, con el SId 76 Hex, el TREP 02 Hex y el método adecuado de división y recuento de submensajes:

Estructura de datos de primera generación

Elemento de dato	Observaciones
TimeReal	Fecha del día transferido
OdometerValueMidnight	Odómetro al final del día transmitido
VuCardIWData	Datos de los ciclos de inserción y extracción de las tarjetas. — Si esta sección no contiene datos disponibles, únicamente se envía el mensaje 'noOfVuCardIWRecords=0'. — Cuando un VuCardIWRecord se encuentra en 00:00 (inserción de la tarjeta el día anterior) o en 24:00 (extracción de la tarjeta al día siguiente) figurará por completo en ambos días.
VuActivityDailyData	Estado de las ranuras a las 00:00 y cambios de actividad registrados en el día transferido.
VuPlaceDailyWorkPeriodData	Datos relacionados con lugares registrados en el día transferido. Si esta sección está vacía, únicamente se envía el mensaje 'noOfPlaceRecords=0'.
VuSpecificConditionData	Datos sobre condiciones específicas registrados en el día transferido. Si esta sección está vacía, únicamente se envía el mensaje 'noOfSpecificConditionRecords=0'.
Signature	Firma RSA de todos los datos desde TimeReal hasta el último byte del último registro de condiciones específicas.

Estructura de datos de segunda generación

Elemento de dato	Observaciones
DateOfDayDownloadedRecordArray	Fecha del día transferido
OdometerValueMidnightRecordArray	Odómetro al final del día transmitido
VuCardIWRecordArray	Datos de los ciclos de inserción y extracción de las tarjetas. — Si esta sección no contiene datos disponibles, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'. — Cuando un VuCardIWRecord se encuentra en 00:00 (inserción de la tarjeta el día anterior) o en 24:00 (extracción de la tarjeta al día siguiente) figurará por completo en ambos días.
VuActivityDailyRecordArray	Estado de las ranuras a las 00:00 y cambios de actividad registrados en el día transferido.
VuPlaceDailyWorkPeriodRecordArray	Datos relacionados con lugares registrados en el día transferido. Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
VuGNSSCDRecordArray	Posiciones GNSS del vehículo si el número de horas de conducción ininterrumpida del conductor alcanza un múltiplo de tres. Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
VuSpecificConditionRecordArray	Datos sobre condiciones específicas registrados en el día transferido. Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
SignatureRecordArray	La firma ECC de todos los datos anteriores.

2.2.6.3 Respuesta positiva a la petición de transferencia de datos sobre incidentes y fallos

DDP_031 El campo de datos del mensaje Positive Response Transfer Data Events and Faults (respuesta positiva a la petición de transferencia de datos sobre incidentes y fallos) contiene los datos siguientes en este orden, con el SId 76 Hex, el TREP 03 Hex y el método adecuado de división y recuento de submensajes:

Estructura de datos de primera generación

Elemento de dato	Observaciones
VuFaultData	Todos los fallos almacenados o en curso en la VU. Si esta sección está vacía, únicamente se envía el mensaje 'noOfVuFaults=0'.
VuEventData	Todos los incidentes almacenados o en curso en la VU (excepto excesos de velocidad). Si esta sección está vacía, únicamente se envía el mensaje 'noOfVuEvents=0'.
VuOverSpeedingControlData	Datos relacionados con el último control de exceso de velocidad (valor por defecto si no se dispone de datos)
VuOverSpeedingEventData	Todos los registros de exceso de velocidad almacenados en la VU. Si esta sección está vacía, únicamente se envía el mensaje 'noOfVuOverSpeedingEvents=0'.
VuTimeAdjustmentData	Todos los incidentes de sincronización almacenados en la VU (fuera del marco de un calibrado total). Si esta sección está vacía, únicamente se envía el mensaje 'noOfVuTimeAdjRecords=0'.
Signature	Firma RSA de todos los datos desde noOfVuFaults hasta el último byte del último registro de ajustes temporales.

Estructura de datos de segunda generación

Elemento de dato	Observaciones
VuFaultRecordArray	Todos los fallos almacenados o en curso en la VU. Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
VuEventRecordArray	Todos los incidentes almacenados o en curso en la VU (excepto excesos de velocidad). Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
VuOverSpeedingControlDataRecordArray	Datos relacionados con el último control de exceso de velocidad (valor por defecto si no se dispone de datos)
VuOverSpeedingEventRecordArray	Todos los registros de exceso de velocidad almacenados en la VU. Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
VuTimeAdjustmentRecordArray	Todos los incidentes de sincronización almacenados en la VU (fuera del marco de un calibrado total). Si esta sección está vacía, se envía una cabecera de conjunto con el mensaje 'noOfRecords=0'.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	La firma ECC de todos los datos anteriores.

2.2.6.4 Respuesta positiva a la petición de transferencia de datos pormenorizados sobre la velocidad

DDP_032 El campo de datos del mensaje Positive Response Transfer Data Detailed Speed (respuesta positiva a la petición de transferencia de datos detallados sobre la velocidad) contiene los datos siguientes en este orden, con el SId 76 Hex, el TREP 04 Hex y el método adecuado de división y recuento de submensajes:

Estructura de datos de primera generación

Elemento de dato	Observaciones
VuDetailedSpeedData	Todos los datos de velocidad detallados almacenados en la VU (un bloque de velocidad por minuto de movimiento del vehículo). 60 valores de velocidad por minuto (uno por segundo).
Signature	Firma RSA de todos los datos desde noOfSpeedBlocks hasta el último byte del último bloque de velocidad.

Estructura de datos de segunda generación

Elemento de dato	Observaciones
VuDetailedSpeedBlockRecordArray	Todos los datos de velocidad detallados almacenados en la VU (un bloque de velocidad por minuto de movimiento del vehículo). 60 valores de velocidad por minuto (uno por segundo).
SignatureRecordArray	La firma ECC de todos los datos anteriores.

2.2.6.5 Respuesta positiva a la petición de transferencia de datos técnicos

DDP_033 El campo de datos del mensaje Positive Response Transfer Data Technical Data (respuesta positiva a la petición de transferencia de datos técnicos) contiene los datos siguientes en este orden, con el SId 76 Hex, el TREP 05 Hex y el método adecuado de división y recuento de submensajes:

Estructura de datos de primera generación

Elemento de dato	Observaciones
VuIdentification	
SensorPaired	
VuCalibrationData	Todos los registros de calibrado almacenados en la VU.
Signature	Firma RSA de todos los datos desde vuManufacturerName hasta el último byte del último VuCalibrationRecord.

Estructura de datos de segunda generación

Elemento de dato	Observaciones
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Todos los emparejamientos de los Estados miembros almacenados en la VU.
VuSensorExternalGNSSCoupledRecordArray	Todos los emparejamientos de la dispositivo GNSS externo almacenados en la VU.
VuCalibrationRecordArray	Todos los registros de calibrado almacenados en la VU.
VuCardRecordArray	Todos los datos de inserción de tarjeta almacenados en la VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	La firma ECC de todos los datos anteriores.

2.3. **Almacenamiento de un archivo en un ESM**

DDP_034 Si una sesión de transferencia ha incluido una transferencia de datos de la VU, el IDE deberá almacenar en un único archivo físico todos los datos recibidos de la VU durante dicha sesión de transferencia dentro de los mensajes de respuesta positiva a la solicitud de transferencia. Los datos almacenados excluyen las cabeceras de mensajes, los contadores de submensajes, los submensajes vacíos y las sumas de control, pero incluyen el SId y el TREP (del primer submensaje exclusivamente si es que hay varios submensajes).

3. PROTOCOLO DE TRANSFERENCIA DE LOS DATOS ALMACENADOS EN TARJETAS DE TACÓGRAFO

3.1. **Ámbito de aplicación**

El presente apartado describe cómo se transfieren directamente a un IDE los datos almacenados en una tarjeta de tacógrafo. El IDE no forma parte del entorno seguro, por tanto no se lleva a cabo una autenticación entre la tarjeta y el IDE.

3.2. **Definiciones**

Sesión de transferencia: Cada vez que se transfieren los datos de la ICC. Esta sesión comprende el procedimiento completo desde el reinicio de la ICC por parte de un IFD hasta la desactivación de la ICC (extracción de la tarjeta o siguiente reinicio).

Archivo de datos firmado: Un archivo de la ICC. El archivo se transfiere al IFD en forma de texto. En la ICC, el archivo se somete a una comprobación aleatoria y se firma, y la firma se transfiere al IFD.

3.3. **Transferencia de los datos de la tarjeta**

DDP_035 La transferencia de los datos de una tarjeta de tacógrafo consta de los pasos siguientes:

— Transferencia de la información común de la tarjeta almacenada en los archivos EF ICC e IC. Esta información es opcional y no se protege con una firma digital.

— Transferencia de los archivos EF Card_Certificate (o CardSignCertificate) y CA_Certificate. Esta información no se protege con una firma digital.

Es obligatorio transferir estos archivos para cada sesión de transferencia.

— Transferencia del resto de archivos EF con datos de aplicación (dentro del archivo Tachograph DF y Tachograph_G2 DF, si existe) excepto el EF Card_Download. Esta información se protege con una firma digital.

— Es obligatorio transferir al menos los archivos EF Application_Identification e ID para cada sesión de transferencia.

— Cuando se transfieran los datos de una tarjeta del conductor, también es obligatorio transferir los siguientes archivos EF:

- `Events_Data`,
- `Faults_Data`,
- `Driver_Activity_Data`,
- `Vehicles_Used`,
- `Places`,
- `GNSS_Places (si existe)`,
- `Control_Activity_Data`, y
- `Specific_Conditions`.

— Cuando se transfieran los datos de una tarjeta del conductor, se actualizará la fecha `LastCardDownload` en el archivo EF `Card_Download`.

— Cuando se transfieran los datos de una tarjeta de taller, habrá que reiniciar el contador de calibrado en el archivo EF `Card_Download`.

— Al transferir una tarjeta de taller, no debe transferirse `EF Sensor_Installation_Data`.

3.3.1 *Secuencia de inicialización*

DDP_036 El IDE deberá iniciar la secuencia de la manera siguiente:

Tarjeta	Dirección	IDE/IFD	Significado/Observaciones
	⇦	Reinicio de hardware	
ATR	⇨		

Opcionalmente se puede utilizar PPS para cambiar a una velocidad en baudios más alta, siempre y cuando la admita la ICC.

3.3.2 *Secuencia para archivos de datos no firmados*

DDP_037 A continuación se muestra la secuencia para transferir los archivos EF ICC, IC, Card_Certificate (o CardSignCertificate) y CA_Certificate:

Tarjeta	Dirección	IDE/IFD	Significado/Observaciones
	⇦	**Select File (seleccionar archivo)**	Selección de archivo utilizando su identificador.
OK	⇨		
	⇦	**Read Binary (leer archivo binario)**	Si el archivo contiene más datos de los que caben en la memoria temporal del lector o de la tarjeta, habrá que repetir el comando hasta que se haya leído el archivo completo.
File Data (datos del archivo) **OK**	⇨	Almacenar datos en un ESM	según lo previsto en el apartado **3.4** Data storage format

Nota 1: antes de seleccionar el archivo EF Card_Certificate (o CardSignCertificate), es preciso seleccionar la aplicación de tacógrafo (selección por AID).

Nota 2: también es posible seleccionar y leer un archivo en un solo paso al utilizar un comando Read Binary con un identificador EF corto.

3.3.3 *Secuencia para archivos de datos firmados*

DDP_038 La siguiente secuencia debe utilizarse para cada uno de los archivos siguientes que debe transferirse junto con su firma:

Tarjeta	Dir	IDE/IFD	Significado/Observaciones
	⇦	**Select File (seleccionar archivo)**	
OK	⇨		
	⇦	**Perform Hash of File (realizar comprobación aleatoria de archivo)**	Calcula el valor de comprobación aleatoria con los datos contenidos en el archivo seleccionado, utilizando el algoritmo de comprobación aleatoria especificado en el apéndice 11. Este no es un comando ISO.
Realizar una comprobación aleatoria del archivo y almacenar temporalmente el valor obtenido			
OK	⇨		
	⇦	**Read Binary (leer archivo binario)**	Si el archivo contiene más datos de los que caben en la memoria temporal del lector o de la tarjeta, habrá que repetir el comando hasta que se haya leído el archivo completo
File Data (datos del archivo) **OK**	⇨	Almacenar los datos recibidos en un ESM	según lo previsto en el apartado **3.4** Data storage format
	⇦	**PSO: Compute Digital Signature (calcular firma digital)**	
Realizar la operación de seguridad «calcular firma digital» utilizando el valor de comprobación aleatoria almacenado temporalmente			
Signature (firma) **OK**	⇨	Añadir datos a los datos previamente almacenados en el ESM	según lo previsto en el apartado **3.4** Data storage format

Nota: también es posible seleccionar y leer un archivo en un solo paso al utilizar un comando Read Binary con un identificador EF corto. En este caso, se podrá seleccionar y leer el EF antes de ejecutar el comando Perform Hash of File (realizar comprobación aleatoria de archivo).

3.3.4 *Secuencia para reiniciar el contador del calibrado*

DDP_039 A continuación se muestra la secuencia para reiniciar el contador `NoOfCalibrationsSinceDownload` en el archivo EF `Card_Download` incluido en una tarjeta del taller:

Tarjeta	Dir	IDE/IFD	Significado/Observaciones
	⇦	**Select File** (seleccionar archivo) EF Card_Download	Selección de archivo utilizando su identificador
OK	⇨		

Tarjeta	Dir	IDE/IFD	Significado/Observaciones
	⇦	**Update Binary (actualizar archivo binario)** NoOfCalibrationsSince-Download=00 00	
Reinicia el número de transferencia de la tarjeta			
OK	⇨		

Nota: también es posible seleccionar y actualizar un archivo en un solo paso al utilizar un comando Update Binary con un identificador EF corto.

3.4. Formato de almacenamiento de datos

3.4.1 *Introducción*

DDP_040 Los datos transferidos deben almacenarse de acuerdo con las siguientes condiciones:

— Los datos almacenados deben ser transparentes. Es decir, durante el almacenamiento es preciso respetar el orden de los bytes que se transfieren de la tarjeta, así como el orden de los bits contenidos en cada byte.

— Todos los archivos de la tarjeta cuyos datos se transfieren en una sesión se almacenan en un archivo dentro del ESM.

3.4.2 *Formato de archivo*

DDP_041 El formato de archivo es una concatenación de varios objetos TLV.

DDP_042 La etiqueta de un EF consiste en el FID más la terminación «00».

DDP_043 La etiqueta de la firma de un EF consiste en el FID del archivo más la terminación «01».

DDP_044 La longitud es un valor de dos bytes. Este valor define el número de bytes en el campo de valor. El valor «FF FF» en el campo de longitud se reserva para uso futuro.

DDP_045 Si un archivo no se transfiere, no deberá almacenarse ninguna información relacionada con dicho archivo (ni la etiqueta ni la longitud cero).

DDP_046 Inmediatamente después del objeto TLV que contiene los datos del archivo, habrá que almacenar una firma como el siguiente objeto TLV.

Definición	Significado	Longitud
FID (2 bytes) || 00	Etiqueta para EF (FID)	3 bytes
FID (2 bytes) || 01	Etiqueta para firma de EF (FID)	3 bytes
xx xx	Longitud del campo de valor	2 bytes

Ejemplo de datos en un archivo transferido y almacenado en un ESM:

Etiqueta	Longitud	Valor
00 02 00	00 11	Datos del archivo EF ICC
C1 00 00	00 C2	Datos del archivo EF Card_Certificate
		…
05 05 00	0A 2E	Datos del archivo EF Vehicles_Used
05 05 01	00 80	Firma del archivo Vehicles_Used

4. TRANSFERENCIA DE LOS DATOS DE UNA TARJETA DE TACÓGRAFO A TRAVÉS DE UNA UNIDAD INSTALADA EN EL VEHÍCULO.

DDP_047 La VU debe permitir la transferencia del contenido de una tarjeta de conductor insertada en un IDE conectado.

DDP_048 El IDE deberá enviar a la VU el mensaje Transfer Data Request Card Download (petición de transferencia de datos de la tarjeta) para iniciar este modo (véase el apartado 2.2.2.9).

DDP_049 A continuación, la VU deberá transferir todos los datos de la tarjeta, archivo por archivo, de acuerdo con el protocolo de transferencia descrito en el apartado 3, para luego enviar al IDE todos los datos recibidos de la tarjeta. Estos datos se enviarán con el formato adecuado de archivo TLV (véase el apartado 3.4.2) y encapsulados en un mensaje Positive Response Transfer Data (respuesta positiva a la petición de transferencia de datos).

DDP_050 El IDE deberá recuperar los datos contenidos en el mensaje Positive Response Transfer Data (respuesta positiva a la petición de transferencia de datos) (separando todas las cabeceras, SId, TREP, contadores de submensajes y sumas de control) y almacenarlos en un único archivo físico, tal y como se especifica en el apartado 2.3.

DDP_051 A continuación, según proceda, la VU actualizará el archivo `Control_Activity_Data` o el archivo `Card_Download` de la tarjeta del conductor.

Apéndice 8

PROTOCOLO DE CALIBRADO

ÍNDICE

1. INTRODUCCIÓN

El presente apéndice define el modo en que se intercambian datos entre una unidad instalada en el vehículo y un verificador a través de la línea K que forma parte de la interfaz de calibrado descrita en el apéndice 6. Asimismo, se explica el control de la línea de señal de entrada/salida en el conector de calibrado.

El establecimiento de las comunicaciones con una línea K se describe en el apartado 4 (Servicios de comunicación).

Este apéndice utiliza la idea de «sesiones de diagnóstico» para determinar el alcance del control de línea K en diferentes condiciones. La sesión por defecto es la «StandardDiagnosticSession», en la que todos los datos se pueden leer desde una unidad instalada en el vehículo pero no es posible escribir ningún dato en ella.

La selección de la sesión de diagnóstico se explica en el apartado 5 (Servicios de administración).

El presente apéndice debe considerarse aplicable tanto para la generación de VU como de tarjetas de taller, según lo previsto en los requisitos de interoperabilidad recogidos en el presente Reglamento.

CPR_001 La «ECUProgrammingSessions» permite la introducción de datos en la unidad instalada en el vehículo. Si se introducen datos de calibrado, la unidad deberá estar además en el modo de funcionamiento CALIBRADO.

La transferencia de datos a través de la línea K se describe en el apartado 6 (Servicios de transmisión de datos). Los formatos de los datos transferidos se detallan en el apartado 8 (Formatos dataRecords).

CPR_002 La «ECUAdjustmentSession» permite seleccionar el modo I/O de la línea de señal I/O de calibrado a través de la interfaz de la línea K. El procedimiento de control de la línea de señal I/O de calibrado se describe en el apartado 7 (Control de los impulsos de prueba — Unidad funcional para control de entrada/salida).

CPR_003 En todo el documento se hace referencia a la dirección del verificador como «tt». A pesar de que puedan existir direcciones preferentes para los verificadores, la VU deberá responder correctamente a cualquier dirección de verificador. La dirección física de la VU es 0xEE.

2. TÉRMINOS, DEFINICIONES Y REFERENCIAS

Todos los protocolos, mensajes y códigos de error se rigen principalmente por el proyecto de la norma ISO 14229-1 (Vehículos de carretera — Sistemas de diagnóstico — Parte 1: Servicios de diagnóstico, versión de 6 de 22 de febrero de 2001).

Se emplea la codificación de bytes y los valores hexadecimales para los identificadores de servicios, las peticiones y respuestas de servicio y los parámetros normalizados.

El término «verificador» se refiere al equipo empleado para introducir datos de programación/calibrado en la VU.

Los términos «cliente» y «servidor» se refieren al verificador y a la VU, respectivamente.

El término UCE significa «unidad de control electrónico» y se refiere a la VU.

Referencias:

ISO 14230-2: Vehículos de carretera — Sistemas de diagnóstico — Protocolo Keyword 2000 — Parte 2: Nivel de enlace de datos.

Primera edición: 1999.

Vehículos — Diagnóstico.

3. VISIÓN GENERAL DE LOS SERVICIOS

3.1. **Servicios disponibles**

La siguiente tabla ofrece una visión general de los servicios que estarán disponibles en el tacógrafo y que se definen en el presente documento.

CPR_004 La tabla indica los servicios que están disponibles en una sesión de diagnóstico activada.

— La **primera columna** especifica los servicios que están disponibles.

— La **segunda columna** incluye el número del apartado del presente apéndice donde se ofrece más información sobre el servicio que corresponda.

— La **tercera columna** asigna los valores de identificador de servicio (SId) para los mensajes de petición.

— La **cuarta columna** especifica los servicios de la «**StandardDiagnosticSession**» **(SD)** que deben aplicarse en cada VU.

— La **quinta columna** especifica los servicios de la «**ECUAdjustmentSession**» **(ECUAS)** que deben aplicarse para poder controlar la línea de señal I/O en el conector de calibrado de la VU, situado en el panel frontal.

— La **sexta columna** especifica los servicios de la «**ECUProgrammingSession**» **(ECUPS)** que deben aplicarse para poder programar los parámetros en la VU.

Tabla 1

Cuadro resumen con los valores de los identificadores de servicios

			Sesiones de diagnóstico		
Nombre del servicio de diagnóstico	Sección nº	Valor SId de la petición	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
Testerpresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Este símbolo indica que el servicio es obligatorio en esa sesión de diagnóstico.

La ausencia de símbolo indica que el servicio no se admite en esa sesión de diagnóstico.

3.2. **Códigos de respuesta**

Se definen los códigos de respuesta para cada servicio.

4. SERVICIOS DE COMUNICACIÓN

Se requieren ciertos servicios para establecer y mantener la comunicación, y no aparecen en el nivel de aplicación. Los servicios disponibles se describen con detalle en la siguiente tabla:

Tabla 2

Servicios de comunicación

Nombre del servicio	Descripción
StartCommunication	El cliente solicita el comienzo de una sesión de comunicación con uno o varios servidores.
StopCommunication	El cliente solicita el término de la sesión de comunicación actual.
Testerpresent	El cliente indica al servidor que todavía está presente.

CPR_005 El servicio StartCommunication sirve para comenzar una comunicación. A fin de utilizar un servicio, es preciso inicializar la comunicación y que los parámetros de comunicación sean los adecuados para el modo deseado.

4.1. **Servicio StartCommunication**

CPR_006 Nada más recibir una indicación primitiva StartCommunication, la VU deberá comprobar si el enlace de comunicación solicitado se puede inicializar en las condiciones que haya en ese momento. Las condiciones válidas para la inicialización de un enlace de comunicación se describen en la norma ISO 14230-2.

CPR_007 A continuación, la VU deberá hacer todo lo necesario para inicializar el enlace de comunicación y enviar una primitiva de respuesta StartCommunication con los parámetros de respuesta positiva seleccionados.

CPR_008 Si una VU que ya está inicializada (y ha entrado en una sesión de diagnóstico) recibe una nueva petición StartCommunication Request (por ejemplo, debido a la recuperación de un error en el verificador), la petición será aceptada y la VU se reinicializará.

CPR_009 Si el enlace de comunicación no se puede inicializar por algún motivo, la VU deberá seguir funcionando en el modo que lo estaba haciendo justo antes del intento de inicialización de dicho enlace de comunicación.

CPR_010 Es preciso asignar una dirección física al mensaje StartCommunication Request.

CPR_011 La inicialización de la VU para los servicios se efectúa a través de un método de «inicialización rápida».

— Antes de cualquier actividad hay un tiempo de inactividad del bus.

— A continuación, el verificador envía una pauta de inicialización.

— La respuesta de la VU incluye toda la información necesaria para establecer la comunicación.

CPR_012 Una vez concluida la inicialización:

— todos los parámetros de comunicación se configuran con los valores definidos en la Tabla 4, de acuerdo con los bytes clave;

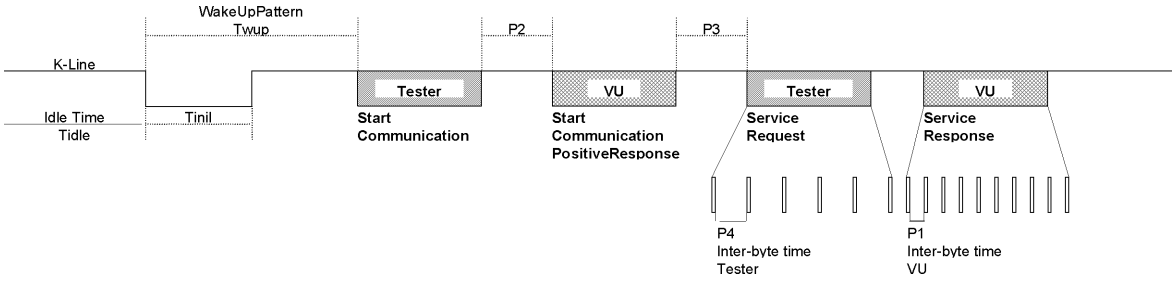
— la VU está esperando la primera petición del verificador;

— la VU se encuentra en el modo de diagnóstico por defecto, es decir, StandardDiagnosticSession; y

— la línea de señal I/O de calibrado se encuentra en el estado por defecto, es decir, desactivada.

CPR_014 La velocidad de datos en la línea K será de 10 400 baudios.

CPR_016 El verificador comienza la inicialización rápida transmitiendo una pauta de activación (Wup) por la línea K. La pauta comienza después del período de reposo de la línea K con un tiempo Tinil breve. El verificador transmite el primer bit del servicio StartCommunication después de un tiempo Twup que sigue al primer flanco descendente.



CPR_017 Los valores de sincronización para la inicialización rápida y las comunicaciones en general se describen con todo detalle en las tablas siguientes. Existen diferentes posibilidades para el tiempo de reposo (Trep):

— primera transmisión después de conectar la alimentación, Trep=300 ms;

— después de haber terminado un servicio StopCommunication, Trep=P3 mín.; y

— después de haberse interrumpido la comunicación por exceso del tiempo límite P3 máx., Trep=0.

Tabla 3

Valores de sincronización para inicialización rápida

Parámetro		Valor mínimo	Valor máximo
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabla 4

valores de sincronización de la comunicación

Sincronización Parámetro	Descripción del parámetro	Valores límite inferiores (ms)	Valores límite superiores (ms)
		mín.	máx.
P1	Tiempo entre dos bytes para respuesta de la VU	0	20
P2	Tiempo transcurrido entre la petición del verificador y la respuesta de la VU o entre dos respuestas de la VU	25	250
P3	Tiempo transcurrido desde el final de las respuestas de la VU hasta el comienzo de la nueva petición del verificador	55	5 000
P4	Tiempo entre dos bytes para petición del verificador	5	20

CPR_018 En las siguientes tablas se describe con detalle el formato de mensaje para inicialización rápida. (NOTA: hex significa hexadecimal)

Tabla 5

Mensaje StartCommunication Request (petición de inicio de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	81	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	**StartCommunication Request Service Id (SId de petición de inicio de la comunicación)**	**81**	**SCR**
Nº 5	Suma de control	00-FF	CS

Tabla 6

mensaje StartCommunication Positive Response (respuesta positiva a la petición de inicio de lacomunicación)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	03	LEN
Nº 5	**StartCommunication Positive Response Service Id (SId de respuesta positiva a la petición de inicio de la comunicación)**	**C1**	**SCRPR**
Nº 6	Byte clave 1	EA	KB1
Nº 7	Byte clave 2	8F	KB2
Nº 8	Suma de control	00-FF	CS

CPR_019 No hay respuesta negativa al mensaje StartCommunication Request. Si no hay un mensaje de respuesta positiva que transmitir, la VU no se inicializa, no transmite ninguna información y continúa en el modo normal de funcionamiento.

4.2. **Servicio StopCommunication**

4.2.1 *Descripción del mensaje*

Este servicio del nivel de comunicación sirve para poner fin a una sesión de comunicación.

CPR_020 Cuando reciba una indicación primitiva StopCommunication, la VU deberá comprobar si las condiciones que haya en ese momento permiten poner término a la comunicación. En caso afirmativo, la VU hará todo lo necesario para terminar la comunicación.

CPR_021 Si es posible poner fin a la comunicación, antes de que esta termine la VU deberá emitir una primitiva de respuesta StopCommunication con los parámetros de respuesta positiva seleccionados.

CPR_022 Si por algún motivo no es posible poner fin a la comunicación, la VU deberá emitir una primitiva de respuesta StopCommunication con el parámetro de respuesta negativa seleccionado.

CPR_023 Si la VU detecta que se ha sobrepasado el tiempo límite P3máx., la comunicación deberá terminar sin que se emita una primitiva de respuesta.

4.2.2 *Formato del mensaje*

CPR_024 En las siguientes tablas se describen con detalle los formatos de mensaje para las primitivas StopCommunication.

Tabla 7

Mensaje StopCommunication Request (petición de interrupción de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	Byte de longitud adicional	01	LEN
Nº 5	**StopCommunication Request Service Id (SId de petición de interrupción de la comunicación)**	**82**	**SPR**
Nº 6	Suma de control	00-FF	CS

Tabla 8

Mensaje StopCommunication Positive Response (respuesta positiva a la petición de interrupción de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	01	LEN
Nº 5	**StopCommunication Positive Response Service Id (SId de respuesta positiva a la petición de interrupción de la comunicación)**	**C2**	**SPRPR**
Nº 6	Suma de control	00-FF	CS

Tabla 9

Mensaje StopCommunication Negative Response (respuesta negativa a la petición de interrupción de la comunicación)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	03	LEN
Nº 5	**negative Response Service Id (SId de respuesta negativa)**	**7F**	**NR**
Nº 6	StopCommunication Request Service Identification (SId de petición de interrupción de la comunicación)	82	SPR
Nº 7	responseCode = generalReject	10	RC_GR
Nº 8	Suma de control	00-FF	CS

4.2.3 *Definición del parámetro*

Este servicio no precisa definición de parámetros.

4.3. **Servicio TesterPresent (presencia de verificador)**

4.3.1 *Descripción del mensaje*

El servicio TesterPresent lo utiliza el verificador para indicar al servidor que sigue presente, con el fin de evitar que retorne automáticamente al funcionamiento normal, lo que podría interrumpir la comunicación. Este servicio, que se envía periódicamente, mantiene activa la comunicación o la sesión de diagnóstico al reiniciar el temporizador P3 cada vez que se recibe una petición de este servicio.

4.3.2 *Formato del mensaje*

CPR_079 En las siguientes tablas se describen con detalle los formatos de mensaje para las primitivas TesterPresent.

Tabla 10

Mensaje TesterPresent Request (petición de presencia de verificador)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	Byte de longitud adicional	02	LEN
Nº 5	**TesterPresent Request Service Id (SId de petición de presencia de verificador)**	**3E**	**TP**

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 6	Sub Function = responseRequired = [sí	01	RESPREQ_Y
	no]	02	RESPREQ_NO
Nº 7	Suma de control	00-FF	CS

CPR_080 Si se configura en «sí» el parámetro responseRequired, el servidor responderá con el mensaje de respuesta positiva siguiente. Si se configura en «no», el servidor no enviará respuesta.

Tabla 11

Mensaje TesterPresent Positive Response (respuesta positiva a la petición de presencia de verificador)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	01	LEN
Nº 5	**TesterPresent Positive Response Service Id (SId de respuesta positiva a la petición de presencia de verificador)**	**7E**	**TPPR**
Nº 6	Suma de control	00-FF	CS

CPR_081 El servicio admitirá los siguientes códigos de respuesta negativa:

Tabla 12

Mensaje TesterPresent Negative Response (respuesta negativa a la petición de presencia de verificador)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	03	LEN
Nº 5	**negative Response Service Id (SId de respuesta negativa)**	**7F**	**NR**
Nº 6	TesterPresent Request Service Identification (SId de petición de presencia de verificador)	3E	TP

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
Nº 8	Suma de control	00-FF	CS

5. SERVICIOS DE ADMINISTRACIÓN

Los servicios disponibles se describen con detalle en la siguiente tabla:

Tabla 13

Servicios de administración

Nombre del servicio	Descripción
StartDiagnosticSession	El cliente solicita el comienzo de una sesión de diagnóstico con una VU.
SecurityAccess	El cliente solicita acceso a las funciones restringidas a usuarios autorizados.

5.1. **Servicio StartDiagnosticSession**

5.1.1 *Descripción del mensaje*

CPR_025 El servicio StartDiagnosticSession sirve para activar diferentes sesiones de diagnóstico en el servidor. Una sesión de diagnóstico activa un conjunto específico de servicios de acuerdo con la Tabla 17. Una sesión puede activar servicios específicos de un fabricante de vehículos que no formen parte del presente documento. Las reglas de aplicación deberán cumplir los siguientes requisitos:

— habrá siempre exactamente una sesión de diagnóstico activa en la VU;

— la VU iniciará siempre la StandardDiagnosticSession al encendido. Si no se inicia ninguna otra sesión de diagnóstico, se estará ejecutando la StandardDiagnosticSession mientras la VU esté encendida;

— si el verificador solicita una sesión de diagnóstico que se está ejecutando ya, la VU enviará un mensaje de respuesta positiva; y

— cuando el verificador solicite una nueva sesión de diagnóstico, la VU enviará primero un mensaje de respuesta positiva StartDiagnosticSession antes de que la nueva sesión se active en la VU. Si la VU no puede iniciar la nueva sesión de diagnóstico solicitada, responderá con un mensaje de respuesta negativa StartDiagnosticSession y proseguirá la sesión ya activa.

CPR_026 Solo se iniciará una sesión de diagnóstico si se ha establecido comunicación entre el cliente y la VU.

CPR_027 Los parámetros de sincronización definidos en la Tabla 4 deberán estar activados tras comenzar la sesión de diagnóstico (StartDiagnosticSession). El parámetro diagnosticSession estará configurado a «StandardDiagnosticSession» (sesión normal) en el mensaje de petición si previamente estaba activada otra sesión de diagnóstico.

5.1.2 *Formato del mensaje*

CPR_028 En las siguientes tablas se describen con detalle los formatos de mensaje para las primitivas StartDiagnosticSession.

Tabla 14

Mensaje StartDiagnosticSession Request (petición de inicio de la sesión de diagnóstico)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	Byte de longitud adicional	02	LEN
Nº 5	**StartDiagnosticSession Request Service Id (SId de petición de inicio de la sesión de diagnóstico)**	**10**	**STDS**
Nº 6	diagnosticSession = [uno de los valores de la Tabla 17]	xx	DS_…
Nº 7	Suma de control	00-FF	CS

Tabla 15

Mensaje StartDiagnosticSession Positive Response (respuesta positiva a la petición de inicio de la sesión dediagnóstico)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	02	LEN
Nº 5	**StartDiagnosticSession Positive Response Service Id (SId de respuesta positiva a la petición de inicio de la sesión de diagnóstico)**	**50**	**STDSPR**
Nº 6	diagnosticSession = [el mismo valor que en el byte nº6 de la Tabla 14]	xx	DS_…
Nº 7	Suma de control	00-FF	CS

Tabla 16

Mensaje StartDiagnosticSession Negative Response (respuesta negativa a la petición de inicio de la sesiónde diagnóstico)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT

Nº de byte	Nombre del parámetro		Valor hex	Mnemónico
Nº 3	Byte de dirección de origen		EE	SRC
Nº 4	Byte de longitud adicional		03	LEN
Nº 5	**Negative Response Service Id (SId de respuesta negativa)**		**7F**	**NR**
Nº 6	StartDiagnosticSession Request Service Id (SId de petición de inicio de la sesión de diagnóstico)		10	STDS
Nº 7	ResponseCode =	[subFunctionNotSupported [a]	12	RC_SFNS
		incorrectMessageLength [b]	13	RC_IML
		conditionsNotCorrect [c]	22	RC_CNC
Nº 8	Suma de control		00-FF	CS

[a] : no se admite el valor introducido en el byte nº 6 del mensaje de petición, puesto que no figura en la Tabla 17.
[b] : la longitud del mensaje es incorrecta.
[c] : no se cumplen los requisitos para la petición StartDiagnosticSession.

5.1.3 *Definición del parámetro*

CPR_029 El servicio StartDiagnosticSession utiliza el parámetro ***diagnosticSession (DS_)*** para seleccionar el comportamiento específico del servidor o servidores. En el presente documento se especifican las siguientes sesiones de diagnóstico:

Tabla 17

Definición de valores de la sesión de diagnóstico

Hex	Descripción	Mnemónico
81	**StandardDiagnosticSession (sesión de diagnóstico normal)** Esta sesión de diagnóstico activa todos los servicios especificados en la **Tabla 1**, **columna 4 (SD)**. Dichos servicios permiten la lectura de datos de un servidor (VU). Esta sesión de diagnóstico se activa después de haber finalizado con éxito la inicialización entre el cliente (verificador) y el servidor (VU). Es posible que otras sesiones de diagnóstico especificadas en este apartado sobrescriban esta sesión de diagnóstico.	**SD**
85	**ECUProgrammingSession (sesión de programación ECUPS)** Esta sesión de diagnóstico activa todos los servicios especificados en la **Tabla 1**, **columna 6 (ECUPS)**. Dichos servicios admiten la programación de memoria de un servidor (VU). Es posible que otras sesiones de diagnóstico especificadas en este apartado sobrescriban esta sesión de diagnóstico.	**ECUPS**
87	**ECUAdjustmentSession (sesión de ajuste ECUA)** Esta sesión de diagnóstico activa todos los servicios especificados en la **Tabla 1**, **columna 5 (ECUAS).** Dichos servicios admiten el control de entrada/salida de un servidor (VU). Es posible que otras sesiones de diagnóstico especificadas en este apartado sobrescriban esta sesión de diagnóstico.	**ECUAS**

5.2. **Servicio SecurityAccess**

No es posible escribir datos de calibrado a menos que la VU se encuentre en el modo CALIBRADO. Para poder acceder al modo CALIBRADO es preciso insertar una tarjeta de taller válida y además introducir el PIN adecuado en la VU.

También se podrá acceder a la línea de entrada/salida de calibrado cuando la VU se encuentre en el modo CALIBRADO o CONTROL.

El servicio SecurityAccess sirve como medio para introducir el PIN y para indicar al verificador si la VU se encuentra o no en el modo CALIBRADO.

El PIN también se puede introducir por otros métodos alternativos.

5.2.1 *Descripción del mensaje*

El servicio SecurityAccess se compone de un mensaje SecurityAccess «requestSeed», seguido en su caso de un mensaje SecurityAccess «sendKey». El servicio SecurityAccess debe utilizarse después del servicio StartDiagnosticSession.

CPR_033 El verificador deberá utilizar el mensaje SecurityAccess «requestSeed» para comprobar si la unidad instalada en el vehículo está preparada para aceptar un PIN.

CPR_034 Si la unidad instalada en el vehículo ya se encuentra en el modo CALIBRADO, deberá contestar a la petición enviando una «simiente» (*seed*) de 0x0000, utilizando para ello el servicio SecurityAccess Positive Response.

CPR_035 Si la unidad instalada en el vehículo está preparada para aceptar un PIN para la verificación por parte de una tarjeta de taller, deberá contestar a la petición enviando una «simiente» (*seed*) mayor que 0x0000, utilizando para ello el servicio SecurityAccess Positive Response.

CPR_036 Si la unidad instalada en el vehículo no está preparada para aceptar un PIN del verificador, ya sea porque la tarjeta de taller que se ha insertado no es válida, o porque no se ha insertado ninguna tarjeta, o porque la unidad espera el PIN de otro método, deberá contestar a la petición con una respuesta negativa, con un código de respuesta configurado a conditionsNotCorrectOrRequestSequenceError.

CPR_037 A continuación, el verificador utilizará en su caso el mensaje SecurityAccess «sendKey» para enviar un PIN a la unidad instalada en el vehículo. A fin de conceder tiempo suficiente para el proceso de autenticación de la tarjeta, la VU utilizará el código de respuesta negativa requestCorrectlyReceived-ResponsePending para ampliar el tiempo de respuesta. Sin embargo, el tiempo de respuesta máximo no excederá de cinco minutos. En cuanto finalice el servicio solicitado, la VU enviará un mensaje de respuesta positiva o un mensaje de respuesta negativa con un código de respuesta distinto de este. La VU podrá repetir el código de respuesta negativa requestCorrectlyReceived-ResponsePending hasta que finalice el servicio solicitado y se envíe el mensaje de respuesta final.

CPR_038 La unidad instalada en el vehículo solamente deberá contestar a esta petición utilizando el servicio SecurityAccess Positive Response cuando se encuentre en el modo CALIBRADO.

CPR_039 En los casos siguientes, la unidad instalada en el vehículo deberá contestar a esta petición con una respuesta negativa con un código de respuesta configurado a:

— subFunctionNotSupported: formato del parámetro de subfunción no válido (accessType);

— conditionsNotCorrectOrRequestSequenceError: la unidad instalada en el vehículo no está lista para aceptar una entrada PIN;

— invalidKey: el PIN no es válido y no se ha sobrepasado el número de intentos de verificación del PIN;

— exceedNumberOfAttempts: el PIN no es válido y se ha sobrepasado el número de intentos de verificación del PIN; y

— generalReject: el PIN es correcto pero ha fallado la autenticación mutua con la tarjeta de taller.

5.2.2 *Formato del mensaje — SecurityAccess — requestSeed*

CPR_040 En las siguientes tablas se describen con detalle los formatos de mensaje para las primitivas SecurityAccess «requestSeed» (petición de simiente).

Tabla 18

Mensaje SecurityAccess Request- requestSeed (petición de simiente)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	Byte de longitud adicional	02	LEN
Nº 5	**SecurityAccess Request Service Id (SId de petición de servicio SecurityAccess)**	**27**	**SA**
Nº 6	accessType — requestSeed	7D	AT_RSD
Nº 7	Suma de control	00-FF	CS

Tabla 19

Mensaje SecurityAccess — requestSeed Positive Response (respuesta positiva a la petición de simiente)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	04	LEN
Nº 5	**SecurityAccess Positive Response Service Id (SId de respuesta positiva a la petición de servicio SecurityAccess)**	**67**	**SAPR**
Nº 6	accessType — requestSeed	7D	AT_RSD
Nº 7	Seed High	00-FF	SEEDH
Nº 8	Seed Low	00-FF	SEEDL
Nº 9	Suma de control	00-FF	CS

Tabla 20

Mensaje SecurityAccess –requestSeed Negative Response (respuesta negativa a la petición de simiente)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 4	Byte de longitud adicional	03	LEN
Nº 5	**NegativeResponse Service Id (SId de respuesta negativa)**	**7F**	**NR**
Nº 6	SecurityAccess Request Service Id (SId de petición de servicio SecurityAccess)	27	SA
Nº 7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
Nº 8	Suma de control	00-FF	CS

5.2.3 *Formato del mensaje — SecurityAccess — sendKey*

CPR_041 En las siguientes tablas se describen con detalle los formatos de mensaje para las primitivas SecurityAccess «sendKey» (envío de clave).

Tabla 21

Mensaje SecurityAccess Request — sendKey (envío de clave)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	Byte de longitud adicional	m+2	LEN
Nº 5	**SecurityAccess Request Service Id (SId de petición de servicio SecurityAccess)**	**27**	**SA**
Nº 6	accessType — sendKey	7E	AT_SK
Nºs 7 a m +6	Clave nº 1 (alto) … Clave nº m (bajo, m debe ser como mínimo 4 y como máximo 8)	xx … xx	CLAVE
Nº m+7	Suma de control	00-FF	CS

Tabla 22

Mensaje SecurityAccess — sendKey Positive Response (respuesta positiva a la petición de envío de clave)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 4	Byte de longitud adicional	02	LEN
Nº 5	**SecurityAccess Positive Response Service Id (SId de respuesta positiva a la petición de servicio SecurityAccess)**	**67**	**SAPR**
Nº 6	accessType — sendKey	7E	AT_SK
Nº 7	Suma de control	00-FF	CS

Tabla 23

Mensaje SecurityAccess Negative Response (respuesta negativa)

Nº de byte	Nombre del parámetro		Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física		80	FMT
Nº 2	Byte de dirección de destino		tt	TGT
Nº 3	Byte de dirección de origen		EE	SRC
Nº 4	Byte de longitud adicional		03	LEN
Nº 5	**NegativeResponse Service Id (SId de respuesta negativa)**		**7F**	**NR**
Nº 6	SecurityAccess Request Service Id (SId de petición de servicio SecurityAccess)		27	SA
Nº 7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
Nº 8	Suma de control		00-FF	CS

6. SERVICIOS DE TRANSMISIÓN DE DATOS

Los servicios disponibles se describen con detalle en la siguiente tabla:

Tabla 24

Servicios de transmisión de datos

Nombre del servicio	Descripción
ReadDataByIdentifier	El cliente solicita la transmisión del valor actual de un registro con acceso mediante recordDataIdentifier.
WriteDataByIdentifier	El cliente solicita la escritura de un registro al que se acceda mediante recordDataIdentifier.

6.1. **Servicio ReadDataByIdentifier**

6.1.1 *Descripción del mensaje*

CPR_050 El cliente utiliza el servicio ReadDataByIdentifier para leer valores de registros de datos de un servidor. Los datos se identifican con un recordDataIdentifier (identificador de datos de registros). El fabricante de la VU es el responsable de que se cumplan las condiciones del servidor cuando se utilice este servicio.

6.1.2 *Formato del mensaje*

CPR_051 En las siguientes tablas se describe con detalle los formatos de mensaje para las primitivas ReadDataByIdentifier.

Tabla 25

Mensaje ReadDataByIdentifier Request (petición de servicio ReadDataByIdentifier)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	Byte de longitud adicional	03	LEN
Nº 5	**ReadDataByIdentifier Request Service Id (SId de petición de servicio ReadDataByIdentifier)**	**22**	**RDBI**
Nos 6 a 7	recordDataIdentifier = [un valor de la Tabla 28]	xxxx	RDI_…
Nº 8	Suma de control	00-FF	CS

Tabla 26

Mensaje ReadDataByIdentifier Positive Response (respuesta positiva a la petición de servicio ReadDataByIdentifier)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	m+3	LEN
Nº 5	**ReadDataByIdentifier Positive Response Service Id (SId de respuesta positiva a la petición de servicio ReadDataByIdentifier)**	**62**	**RDBIPR**
Nos 6 y 7	recordDataIdentifier = [mismo valor que los bytes nos 6 y 7 de la Tabla 25]	xxxx	RDI_…
Nos 8 a m +7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
Nº m+8	Suma de control	00-FF	CS

Tabla 27

Mensaje ReadDataByIdentifier Negative Response (respuesta negativa a la petición de servicio-ReadDataByIdentifier)

Nº de byte	Nombre del parámetro		Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física		80	FMT
Nº 2	Byte de dirección de destino		tt	TGT
Nº 3	Byte de dirección de origen		EE	SRC
Nº 4	Byte de longitud adicional		03	LEN
Nº 5	**NegativeResponse Service Id (SId de respuesta negativa)**		**7F**	**NR**
Nº 6	ReadDataByIdentifier Request Service Id (SId de petición de servicio ReadDataByIdentifier)		22	RDBI
Nº 7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
Nº 8	Suma de control		00-FF	CS

6.1.3 *Definición del parámetro*

CPR_052 El parámetro ***recordDataIdentifier (RDI_)*** incluido en el mensaje ReadDataByIdentifier Request identifica un registro de datos.

CPR_053 La siguiente tabla muestra los valores recordDataIdentifier definidos en el presente documento.

La tabla recordDataIdentifier tiene cuatro columnas y múltiples filas.

— La **primera columna (Hex)** incluye el valor hexadecimal asignado al recordDataIdentifier especificado en la tercera columna.

— La **segunda columna (Elemento de datos)** especifica el elemento de datos del apéndice 1 en el que se basa el recordDataIdentifier (a veces es necesario transcodificar).

— La **tercera columna (Descripción)** especifica el nombre recordDataIdentifier correspondiente.

— La **cuarta columna (Término nemónico)** especifica el término nemónico de este recordDataIdentifier.

Tabla 28

Definición de los valores recordDataIdentifier

Hex	Elemento de dato	Nombre recordDataIdentifier (véase formato en el apartado 8.2)	Mnemónico
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Hex	Elemento de dato	Nombre recordDataIdentifier (véase formato en el apartado 8.2)	Mnemónico
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 El mensaje ReadDataByIdentifier Positive Response utiliza el parámetro ***dataRecord (DREC_)*** para facilitar al cliente (verificador) el valor del registro de datos identificado por el recordDataIdentifier. Los formatos de datos se especifican en el apartado 8. Pueden aplicarse dataRecords de usuario adicionales opcionales, que incluyan datos específicos de la VU, tanto internos como de entrada y salida, pero no se definen en el presente documento.

6.2. **Servicio WriteDataByIdentifier**

6.2.1 *Descripción del mensaje*

CPR_056 El cliente utiliza el servicio WriteDataByIdentifier para escribir valores de registros de datos en un servidor. Los datos se identifican con un recordDataIdentifier (identificador de datos de registros). El fabricante de la VU es el responsable de que se cumplan las condiciones del servidor cuando se utilice este servicio. Para actualizar los parámetros recogidos en la Tabla 28, la VU debe estar en el modo CALIBRADO.

6.2.2 *Formato del mensaje*

CPR_057 En las siguientes tablas se describen con detalle los formatos de mensaje para las primitivas WriteDataByIdentifier.

Tabla 29

Mensaje WriteDataByIdentifier Request (petición de servicio WriteDataByIdentifier)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	Byte de longitud adicional	m+3	LEN
Nº 5	**WriteDataByIdentifier Request Service Id (SId de petición de servicio WriteDataByIdentifier)**	**2E**	**WDBI**
Nºs 6 a 7	recordDataIdentifier = [un valor de la Tabla 28]	xxxx	RDI_…

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 8 a nº m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
Nº m+8	Suma de control	00-FF	CS

Tabla 30

Mensaje WriteDataByIdentifier Positive Response (respuesta positiva a la petición de servicio WriteDataByIdentifier)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	03	LEN
Nº 5	**WriteDataByIdentifier Positive Response Service Id (SId de respuesta positiva a la petición de servicio WriteDataByIdentifier)**	**6E**	**WDBIPR**
Nºs 6 a 7	recordDataIdentifier = [mismo valor que los bytes nºs 6 y 7 de la Tabla 29]	xxxx	RDI_…
Nº 8	Suma de control	00-FF	CS

Tabla 31

Mensaje WriteDataByIdentifier Negative Response (respuesta negativa a la petición de servicio WriteDataByIdentifier)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	03	LEN
Nº 5	**NegativeResponse Service Id (SId de respuesta negativa)**	**7F**	**NR**
Nº 6	WriteDataByIdentifier Request Service Id (SId de petición de servicio WriteDataByIdentifier)	2E	WDBI

Nº de byte	Nombre del parámetro		Valor hex	Mnemónico
Nº 7	ResponseCode =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
Nº 8	Suma de control		00-FF	CS

6.2.3 *Definición del parámetro*

El parámetro ***recordDataIdentifier (RDI_)*** se define en la Tabla 28.

El parámetro ***dataRecord (DREC_)*** lo utiliza el mensaje de petición WriteDataByIdentifier para facilitar al servidor (VU) los valores de registros de datos identificados por el recordDataIdentifier. Los formatos de datos se especifican en el 8.

7. CONTROL DE LOS IMPULSOS DE PRUEBA — UNIDAD FUNCIONAL PARA CONTROL DE ENTRADA/SALIDA

Los servicios disponibles se describen con detalle en la siguiente tabla:

Tabla 32

Unidad funcional para control de entrada/salida

Nombre del servicio	Descripción
InputOutputControlByIdentifier	El cliente solicita el control de una entrada/salida específica del servidor.

7.1. Servicio InputOutputControlByIdentifier

7.1.1 *Descripción del mensaje*

Existe una conexión, a través del conector frontal, que permite controlar o efectuar un seguimiento de los impulsos de prueba utilizando un verificador adecuado.

CPR_058 Esta línea de señal I/O de calibrado se puede configurar con el comando de la línea K empleando el servicio InputOutputControlByIdentifier para seleccionar la función de entrada o salida que se precise para la línea. Los estados de la línea disponibles son:

— desactivado;

— speedSignalInput, donde se utiliza la línea de señal I/O de calibrado para introducir una señal de velocidad (señal de prueba) que sustituye a la señal de velocidad del sensor de movimiento. Esta función no está disponible en el modo CONTROL;

— realTimeSpeedSignalOutputSensor, donde se utiliza la línea de señal I/O de calibrado para extraer la señal de velocidad del sensor de movimiento; y

— RTCOutput, donde se utiliza la línea de señal I/O de calibrado para extraer la señal del reloj de TUC. Esta función no está disponible en el modo CONTROL.

CPR_059 Para configurar el estado de la línea, la unidad instalada en el vehículo tiene que haber entrado en una sesión de ajuste y debe estar en el modo CALIBRADO o CONTROL. Cuando la VU se encuentra en modo CALIBRADO, pueden seleccionarse los cuatro estados de la línea (desactivado, speedSignalInput, realTimeSpeedSignalOutputSensor y RTCOutput). Cuando la VU se encuentra en modo CONTROL, solo pueden seleccionarse dos estados de la línea (desactivado y realTimeSpeedSignalOutputSensor). Al salir de la sesión de ajuste o del modo CALIBRADO o CONTROL, la unidad instalada en el vehículo debe cerciorarse de que la línea de señal I/O vuelve al estado «desactivado» (por defecto).

CPR_060 Si se reciben impulsos de velocidad por la línea de entrada de la VU para señales de velocidad en tiempo real y la línea de señal I/O de calibrado está configurada para transmitir entradas, entonces dicha línea de señal I/O deberá configurarse para transmitir salidas o deberá volver al estado de desactivación.

CPR_061 Se seguirá el orden siguiente:

— establecer comunicación mediante el servicio StartCommunication;

— entrar en una sesión de ajuste mediante el servicio StartDiagnosticSession y estar en el modo CALIBRADO o CONTROL (el orden de estas dos operaciones no es importante); y

— cambiar el estado de la salida mediante el servicio InputOutputControlBylIdentifier.

7.1.2 *Formato del mensaje*

CPR_062 En las siguientes tablas se describen con detalle los formatos de mensaje para las primitivas InputOutputControlByIdentifier.

Tabla 33

Mensaje InputOutputControlByIdentifier Request (petición de control de entrada/salida)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	EE	TGT
Nº 3	Byte de dirección de origen	tt	SRC
Nº 4	Byte de longitud adicional	xx	LEN
Nº 5	**InputOutputControlByIdentifier Request SId (SId de petición de control de entrada/salida)**	**2F**	**IOCBI**
Nºs 6 y 7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
Nº 8 o nºs 8 a 9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter — un valor de la Tabla 36	xx	IOCP_…
	controlState — un valor de la Tabla 37 (véase la nota a continuación)]	xx	CS_…
Nº 9 o 10	Suma de control	00-FF	CS

Nota: el parámetro controlState solo está presente en algunos casos (véase el apartado 7.1.3).

Tabla 34

Mensaje InputOutputControlByIdentifier Positive Response (respuesta positiva a la petición de control deentrada/salida)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	xx	LEN
Nº 5	**inputOutputControlByIdentifier Positive Response SId (SId de respuesta positiva a la petición de control de entrada/salida)**	**6F**	**IOCBIPR**
Nºs 6 y 7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
Nº 8 o nºs 8 a 9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (el mismo valor que en el byte nº8 de la Tabla 33)	xx	IOCP_…
	controlState (mismo valor que byte nº 9 de la Tabla 33)] (en su caso)	xx	CS_…
Nº 9 o 10	Suma de control	00-FF	CS

Tabla 35

Mensaje InputOutputControlByIdentifier Negative Response (respuesta negativa a la petición de control deentrada/salida)

Nº de byte	Nombre del parámetro	Valor hex	Mnemónico
Nº 1	Byte de formato — asignación de dirección física	80	FMT
Nº 2	Byte de dirección de destino	tt	TGT
Nº 3	Byte de dirección de origen	EE	SRC
Nº 4	Byte de longitud adicional	03	LEN
Nº 5	**NegativeResponse Service Id (SId de respuesta negativa)**	**7F**	**NR**
Nº 6	inputOutputControlByIdentifier Request SId (SId de petición de control de entrada/salida)	2F	IOCBI
Nº 7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
Nº 8	Suma de control	00-FF	CS

7.1.3 *Definición del parámetro*

CPR_064 El parámetro ***inputOutputControlParameter (IOCP_)*** se define en la siguiente tabla.

Tabla 36

Definición de los valores inputOutputControlParameter

Hex	Descripción	Mnemónico
00	**ReturnControlToECU** Este valor deberá indicar al servidor (VU) que el verificador ya no tiene control sobre la línea de señal I/O de calibrado.	RCTECU
01	**ResetToDefault** Este valor deberá indicar al servidor (VU) su obligación de reiniciar la señal de I/O de calibrado al estado que le corresponde por defecto.	RTD
03	**ShortTermAdjustment** Este valor deberá indicar al servidor (VU) su obligación de ajustar la línea de señal de I/O de calibrado al valor incluido en el parámetro controlState.	STA

CPR_065 El parámetro ***controlState***, definido en la siguiente tabla, solo está presente cuando el parámetro inputOutputControlParameter se ha configurado a ShortTermAdjustment.

Tabla 37

Definición de valores controlState

Modo	Valor hex	Descripción
Desactivado	00	Línea I/O desactivada (estado por defecto)
Activado	01	Línea I/O de calibrado activada como speedSignalInput
Activado	02	Línea I/O de calibrado activada como realTimeSpeedSignalOutputSensor
Activado	03	Línea I/O de calibrado activada como RTCOutput

8. FORMATOS DATARECORDS

En el presente apartado se detallan:

— las reglas generales que se aplicarán a los intervalos de los parámetros transmitidos por la unidad instalada en el vehículo al verificador; y

— los formatos que se utilizarán en los datos transferidos a través de los servicios de transmisión de datos descritos en el apartado 6.

CPR_067 La VU admitirá todos los parámetros identificados.

CPR_068 Los datos transmitidos por la VU al verificador en respuesta a un mensaje de petición serán del tipo medido (es decir, el valor actual del parámetro solicitado medido u observado por el VU).

8.1. **Intervalos de los parámetros transmitidos**

CPR_069 En la Tabla 38 se definen los intervalos utilizados para determinar la validez de un parámetro transmitido.

CPR_070 Los valores del intervalo «indicador de error» sirven para que la unidad instalada en el vehículo indique inmediatamente que no dispone en ese momento de datos paramétricos válidos por causa de algún tipo de error en el tacógrafo.

CPR_071 Los valores del intervalo «no disponible» sirven para que la unidad instalada en el vehículo transmita un mensaje que contiene un parámetro que no está disponible o no está admitido en ese módulo. Los valores del intervalo «no solicitado» constituyen un medio para que un dispositivo transmita un mensaje de comando e identifique para qué parámetros no se espera respuesta del dispositivo receptor.

CPR_072 Si el fallo de un componente impide la transmisión de datos válidos para un parámetro, deberá utilizarse en lugar de dichos datos el indicador de error descrito en la Tabla 38. Sin embargo, si los datos medidos o calculados adquieren un valor que es válido, pero que excede del intervalo definido para el parámetro, no se utilizará el indicador de error. Se transmitirán los datos utilizando el valor mínimo o máximo del parámetro según proceda.

Tabla 38

Intervalos dataRecords

Nombre del intervalo	1 byte (valor hex)	2 bytes (valor hex)	4 bytes (Valor hex)	ASCII
Señal válida	00 a FA	0000 a FAFF	00000000 a FAFFFFFF	1 a 254
Indicador específico del parámetro	FB	FB00 a FBFF	FB000000 a FBFFFFFF	ninguno
Reservado para futuros bits de indicador	FC a FD	FC00 a FDFF	FC000000 a FDFFFFFF	ninguno
Indicador de error	FE	FE00 a FEFF	FE000000 a FEFFFFFF	0
No disponible o no solicitado	FF	FF00 a FFFF	FF000000 a FFFFFFFF	FF

CPR_073 Para los parámetros codificados en ASCII, el carácter ASCII «*» está reservado como delimitador.

8.2. **Formatos dataRecords**

De la Tabla 39 a la Tabla 42 se detallan los formatos que se usarán a través de los servicios ReadDataByIdentifier y WriteDataByIdentifier.

CPR_074 En la Tabla 39 se ofrece la longitud, resolución e intervalo operativo de cada parámetro, identificado por su recordDataIdentifier:

Tabla 39

Formato de dataRecords

Nombre del parámetro	Longitud de dato (bytes)	Resolución	Intervalo operativo
TimeDate	8	Véanse los detalles en la Tabla 40	
HighResolutionTotalVehicleDistance	4	avance 5 m/bit, inicio 0 m	0 a + 21 055 406 km
Kfactor	2	avance 0,001 pulsos/m/bit, inicio 0	0 a 64,255 pulsos/m
LfactorTyreCircumference	2	avance 0,125 10^{-3} m /bit, inicio 0	0 a 8,031 m
WvehicleCharacteristicFactor	2	avance 0,001 pulsos/m/bit, inicio 0	0 a 64,255 pulsos/m
TyreSize	15	ASCII	ASCII

Nombre del parámetro	Longitud de dato (bytes)	Resolución	Intervalo operativo
NextCalibrationDate	3	Véanse los detalles en la Tabla 41	
SpeedAuthorised	2	avance 1/256 km/h/bit, inicio 0	0 a 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Véanse los detalles en la Tabla 42	
VIN	17	ASCII	ASCII

CPR_075 En la Tabla 40 se detallan los formatos de los distintos bytes del parámetro TimeDate:

Tabla 40

Formato detallado de TimeDate (valor recordDataIdentifier # F90B)

Byte	Definición del parámetro	Resolución	Intervalo operativo
1	Segundos	avance 0,25 s/bit, inicio 0 s	0 a 59,75 s
2	Minutos	avance 1 min/bit, inicio 0 min	0 a 59 min
3	Horas	avance 1 h/bit, inicio 0 h	0 a 23 h
4	Mes	avance 1 mes/bit, 0 mes	1 a 12 meses
5	Día	avance 0,25 día/bit, 0 día (véase la nota de la Tabla 41)	0,25 a 31,75 días
6	Año	avance 1 año/bit, año + 1985 (véase la nota de la Tabla 41)	año 1985 a 2235
7	Local Minute Offset	avance 1 min/bit, inicio − 125 min	− 59 a + 59 min
8	Local Hour Offset	avance 1 h/bit, inicio − 125 h	− 23 a + 23 h

CPR_076 En la Tabla 41 se detallan los formatos de los distintos bytes del parámetro NextCalibrationDate:

Tabla 41

Formato detallado de NextCalibrationDate (valor recordDataIdentifier # F922)

Byte	Definición del parámetro	Resolución	Intervalo operativo
1	Mes	avance 1 mes/bit, 0 mes	1 a 12 meses
2	Día	avance 0,25 día/bit, 0 día (véase la nota a continuación)	0,25 a 31,75 días
3	Año	avance 1 año/bit, año + 1985 (véase la nota a continuación)	año 1985 a 2235

Nota relativa al uso del parámetro «Día»:

1) el valor 0 para la fecha es nulo. Los valores 1, 2, 3 y 4 se utilizan para identificar el primer día del mes; 5, 6, 7 y 8 para el segundo; etc.

2) Este parámetro no influye el parámetro de horas ni lo modifica.

Nota relativa al uso del parámetro «Año»:

el valor 0 para el año identifica el año 1985; el valor 1, el año 1986; etc.

CPR_078 En la Tabla 42 se detallan los formatos de los distintos bytes del parámetro VehicleRegistrationNumber:

Tabla 42

Formato detallado de VehicleRegistrationNumber (valor recordDataIdentifier # F97E)

Byte	Definición del parámetro	Resolución	Intervalo operativo
1	Página de código (según se define en el apéndice 1)	ASCII	01 a 0A
2 — 14	Número de registro del vehículo (según se define en el apéndice 1)	ASCII	ASCII

Apéndice 9.

HOMOLOGACIÓN LISTA DE PRUEBAS MÍNIMAS REQUERIDAS

ÍNDICE

1. INTRODUCCIÓN

1.1. **Homologación**

La homologación CE de un aparato de control (o componente) o de una tarjeta de tacógrafo se basa en:

— una **certificación de seguridad** basada en criterios comunes especificados para acreditar el cumplimiento de un objetivo de seguridad conforme al apéndice 10 del presente anexo (a completar/modificar);

— una **certificación funcional**, realizada por una autoridad de un Estado miembro, para certificar que el elemento sujeto a verificación cumple los requisitos del presente anexo en cuanto a las funciones que desempeña, la exactitud de medición y las características medioambientales; y

— una **certificación de interoperabilidad**, realizada por un organismo competente, para garantizar que el aparato de control (o la tarjeta de tacógrafo) puede interoperar sin restricciones con los modelos necesarios de tarjeta de tacógrafo (o aparato de control) (véase el apartado 8 del presente anexo).

En el presente apéndice se especifican las pruebas mínimas que debe realizar la autoridad del Estado miembro durante los ensayos funcionales, así como las pruebas mínimas que debe realizar el organismo competente durante los ensayos de interoperabilidad. No se determina el tipo de pruebas ni los procedimientos a seguir durante las mismas.

El presente apéndice no se ocupa de los aspectos relativos a la certificación de seguridad. Si durante la evaluación de seguridad y el proceso de certificación se llevan a cabo algunas de las pruebas exigidas para la homologación, no habrá que repetirlas posteriormente. En ese caso, tan solo se comprobarán los resultados de dichas pruebas de seguridad. A título informativo, en el presente apéndice hemos marcado con un asterisco («*») las condiciones que es preciso verificar (y también las condiciones estrechamente asociadas con pruebas que deban realizarse) durante la certificación de seguridad.

Los requisitos numerados se refieren al contenido de este anexo, mientras que el resto de requisitos se refieren al resto de apéndices (por ejemplo, PIC_001 se refiere al requisito PIC_001 del apéndice 3 (pictogramas)).

El presente apéndice trata por separado la homologación del sensor de movimiento, de la unidad instalada en el vehículo y del dispositivo GNSS externo como componentes del aparato de control. Cada uno de los componentes recibirá un certificado de homologación propio, en el que se indicarán el resto de componentes compatibles. La prueba de funcionalidad del sensor de movilidad (o del dispositivo GNSS externo) se realiza junto con la unidad instalada en el vehículo, y al contrario.

No se requiere interoperabilidad entre el sensor de movimiento (o el dispositivo GNSS externo) y cada modelo de la unidad instalada en el vehículo. En este caso, únicamente puede concederse la homologación de un sensor de movimiento (o de un dispositivo GNSS externo) en combinación con el tipo de aprobación de la unidad instalada en el vehículo pertinente, y al contrario.

1.2. **Referencias**

En el presente apéndice aparecen las siguientes referencias:

IEC 60068-2-1: Verificación medioambiental — Parte 2-1: Pruebas — Prueba A: Frío.

IEC 60068-2-2: Procedimientos básicos de verificación medioambiental; Parte 2: pruebas; Prueba B: Calor seco (sinusoidal).

IEC 60068-2-6: Verificación medioambiental — Parte 2: Pruebas — Prueba Fc: Vibración.

IEC 60068-2-14: Verificación medioambiental — Parte 2-14: Pruebas — Prueba N: Variaciones de la temperatura.

IEC 60068-2-27: Pruebas ambientales Parte 2: Pruebas. Prueba Ea y orientación: Choque.

IEC 60068-2-30: Verificación medioambiental — Parte 2-30: Pruebas — Prueba Db: Calor húmedo, cíclico (ciclo de 12 + 12 horas).

IEC 60068-2-64: Verificación medioambiental — Parte 2-64: Pruebas — Prueba Fh: Vibración, aleatorio de banda ancha y orientación.

IEC 60068-2-78 Verificación medioambiental — Parte 2-78: Pruebas — Prueba Cab: Calor húmedo, estado estable.

ISO 16750-3 Cargas mecánicas (2012-12).

ISO 16750-4 Cargas climáticas (2010-04).

ISO 20653: Vehículos de carretera — Niveles de protección (código IP) — Protección del equipo eléctrico frente a objetos extraños, al agua y al acceso.

ISO 10605:2008 + Corrigendum técnico 2010 + AMD1: 2014 Vehículos de carretera — Métodos de prueba para perturbaciones eléctricas por descarga electrostática.

ISO 7637-1:2002 + AMD1: 2008 Vehículos de carretera — Perturbaciones eléctricas por conducción y acoplamiento — Parte 1: Definiciones y consideraciones generales.

ISO 7637-2 Vehículos de carretera — Perturbaciones eléctricas por conducción y acoplamiento — Parte 2: Conducción eléctrica transitoria por líneas de alimentación exclusivamente.

ISO 7637-3 Vehículos de carretera — Perturbaciones eléctricas por conducción y acoplamiento — Parte 3: Transmisión eléctrica transitoria mediante acoplamiento capacitivo e inductivo por líneas que no sean de alimentación.

ISO/IEC 7816-1 Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 1: Características físicas.

ISO/IEC 7816-2 Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 2: Dimensiones y ubicación de los contactos.

ISO/IEC 7816-3 Tecnología de la información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos –Parte 3: Señales electrónicas y protocolo de transmisión.

ISO/IEC 10373-1:2006 + AMD1:2012 Tarjetas de identificación — Métodos de prueba — Parte 1: Características generales

ISO/IEC 10373-3:2010 + Corrigendum técnico 2013 Tarjetas de identificación — Métodos de prueba — Parte 3: Tarjetas de circuitos integrados con contactos y dispositivos de interfaz relacionados

ISO 16844-3:2004, Cor 1:2006 Vehículos de carretera — Sistemas de tacógrafo — Parte 3: Interfaz del sensor de movimiento (con las unidades intravehiculares).

ISO 16844-4 Vehículos de carretera — Sistemas de tacógrafo — Parte 4: Interfaz CAN

ISO 16844-6 Vehículos de carretera — Sistemas de tacógrafo — Parte 6: Diagnóstico

ISO 16844-7 Vehículos de carretera — Sistemas de tacógrafo — Parte 7: Parámetros

ISO 534 Papel y cartón — Fijación del grosor, la densidad y el volumen específico

Reglamento CEPE nº 10 sobre homologación de vehículos respecto a la compatibilidad electromagnética (Comisión Económica para Europa de las Naciones Unidas)

2. PRUEBAS FUNCIONALES DE LA UNIDAD INSTALADA EN EL VEHÍCULO

Nº	Prueba	Descripción	Condiciones correspondientes
1	**Examen administrativo**		
1.1	Documentación	Corrección de la documentación.	
1.2	Resultados de las pruebas del fabricante	Resultados de la prueba realizada por el fabricante durante la integración. Demostraciones sobre papel.	88, 89, 91
2	**Inspección visual**		
2.1	Cumplimiento de lo dispuesto en la documentación		
2.2	Identificación/inscripciones		224 a 226
2.3	Materiales		219 a 223
2.4	Precintos		398, 401 a 405
2.5	Interfaces externas		
3	**Pruebas funcionales**		
3.1	Funciones disponibles		03, 04, 05, 07, 382
3.2	Modos de funcionamiento		09 a 11*, 132, 133
3.3	Funciones y derechos de acceso a los datos		12*, 13*, 382, 383, 386 a 389
3.4	Inserción y extracción de las tarjetas de supervisión		15, 16, 17, 18, 19*, 20*, 132
3.5	Medición de la velocidad y la distancia		21 a 31
3.6	Medición de la hora (ensayo realizado a 20 °C)		38 a 43
3.7	Supervisión de las actividades del conductor		44 a 53, 132
3.8	Supervisión del régimen de conducción		54, 55, 132

Nº	Prueba	Descripción	Condiciones correspondientes
3.9	Entradas manuales		56 a 62
3.10	Gestión de los bloqueos introducidos por las empresas		63 a 68
3.11	Supervisión de las actividades de control		69, 70
3.12	Detección de incidentes o fallos		71 a 88 132
3.13	Datos de identificación del aparato		93*, 94*, 97, 100
3.14	Datos de inserción y extracción de la tarjeta del conductor		102* a 104*
3.15	Datos sobre la actividad del conductor		105* a 107*
3.16	Datos sobre lugares y posiciones		108* a 112*
3.17	Datos del cuentakilómetros		113* a 115*
3.18	Datos pormenorizados sobre la velocidad		116*
3.19	Datos sobre incidentes		117*
3.20	Datos sobre fallos		118*
3.21	Datos de calibrado		119* a 121*
3.22	Datos de ajuste de la hora		124*, 125*
3.23	Datos sobre actividades de control		126*, 127*
3.24	Datos sobre los bloqueos introducidos por las empresas		128*
3.25	Datos sobre actividades de transferencia		129*
3.26	Datos sobre condiciones específicas		130*, 131*
3.27	Registro y almacenamiento de datos en tarjetas de tacógrafo		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Visualización		90, 132, 149 a 166 PIC_001, DIS_001
3.29	Impresión		90, 132, 167 a 179, PIC_001, PRT_001 a PRT_014
3.30	Advertencias		132, 180 a 189, PIC_001

Nº	Prueba	Descripción	Condiciones correspondientes
3.31	Transferencia de datos a medios externos		90, 132, 190 a 194
3.32	Comunicación remota para pruebas en carretera específicas		195 a 197
3.33	Envío de datos a dispositivos externos adicionales		198, 199
3.34	Calibrado		202 a 206*, 383, 384, 386 a 391
3.35	Verificación del calibrado en carretera		207 a 209
3.36	Ajuste de la hora		210 a 212*
3.37	No interferencia con funciones adicionales		06, 425
3.38	Interfaz del sensor de movimiento		02, 122
3.39	Dispositivo GNSS externo		03, 123
3.40	Comprobar si la VU detecta, registra y almacena el o los incidentes o fallos descritos por el fabricante de la VU cuando un sensor de movimiento acoplado reaccione a los campos magnéticos perturbando la detección de movimiento del vehículo.		217
3.41	Serie de cifrado y parámetros de dominio estandarizados		CSM_48, CSM_50
4	**Pruebas ambientales**		
4.1	Temperatura	Verificar la funcionalidad mediante: Prueba en virtud de la ISO 16750-4, apartado 5.1.1.2: prueba de funcionamiento a temperatura baja (72 h a – 20 °C). Esta prueba se refiere a la IEC 60068-2-1: Verificación medioambiental — Parte 2-1: Pruebas — Prueba A: Frío. Prueba en virtud de la ISO 16750-4, apartado 5.1.2.2: prueba de funcionamiento a temperatura alta (72 h a 70 ° C). Esta prueba se refiere a la IEC 60068-2-2: Procedimientos básicos de verificación medioambiental; Parte 2: pruebas; Prueba B: Calor seco. Prueba en virtud de la ISO 16750-4, apartado 5.3.2: cambio rápido de temperatura con una duración de transición específica (– 20 °C/70 °C, 20 ciclos, tiempo: 2 horas en cada temperatura). Es posible llevar a cabo un conjunto reducido de pruebas (de entre las que se definen en la sección 3 de esta tabla) a la temperatura más baja, a la temperatura más alta y durante los ciclos de temperatura.	213

Nº	Prueba	Descripción	Condiciones correspondientes
4.2	Humedad	Verificar que la unidad instalada en el vehículo puede soportar una humedad cíclica (prueba de calor) mediante la norma IEC 60068-2-30, prueba Db, seis ciclos de 24 horas, con una variación de temperatura de + 25 °C a + 55 °C en cada caso y una humedad relativa del 97 % a + 25 °C y del 93 % a + 55 °C.	214
4.3	Mecánica	1. Vibraciones sinusoidales: verificar que la unidad instalada en el vehículo es capaz de soportar vibraciones sinusoidales de las siguientes características: desplazamiento constante entre 5 y 11 Hz: pico de 10 mm; y aceleración constante entre 11 y 300 Hz: 5 g. Esta exigencia se verifica mediante la norma IEC 60068-2-6, prueba Fc, con una duración mínima de 3x12 horas (12 horas por cada eje). La ISO 16750-3 no requiere una prueba de vibración sinusoidal para dispositivos situados en el puesto de conducción del vehículo desacoplado. 2. Vibraciones aleatorias: Prueba en virtud de la ISO 16750-3, apartado 4.1.2.8: prueba VIII: vehículo comercial, puesto de conducción del vehículo desacoplado. Prueba de vibraciones aleatorias, 10-2 000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 3 ejes, 32 horas por eje, incluido un ciclo de temperatura – 20-+ 70 °C. Esta prueba se refiere a la IEC 60068-2-64: Verificación medioambiental — Parte 2-64: Pruebas — Prueba Fh: Vibración, aleatorio de banda ancha y orientación. 3. Choques: choque mecánico con semionda sinusoidal de 3 g de conformidad con la ISO 16750. Las pruebas arriba descritas se llevan a cabo con muestras diferentes del tipo de equipo que se someta a prueba.	219
4.4	Protección frente a la penetración de agua y cuerpos extraños	Prueba en virtud de la ISO 20653: Vehículos de carretera — Niveles de protección (código IP) — Protección del equipo eléctrico frente a objetos extraños, al agua y al acceso (sin cambio en los parámetros); valor mínimo IP 40.	220, 221
4.5	Protección frente a sobretensiones	Verificar que la unidad instalada en el vehículo es capaz de soportar un suministro eléctrico de: versiones de 24 V: 34 V a + 40 °C 1 hora; y versiones de 12 V: 17 V a + 40 °C 1 hora. (ISO 16750-2)	216
4.6	Protección frente a la inversión de la polaridad	Verificar que la unidad instalada en el vehículo es capaz de soportar una inversión de su fuente de alimentación. (ISO 16750-2)	216

Nº	Prueba	Descripción	Condiciones correspondientes
4.7	Protección frente a cortocircuitos	Verificar que las señales de entrada y de salida están protegidas frente a cortocircuitos a la fuente de alimentación y a masa. (ISO 16750-2)	216
5	**Pruebas de compatibilidad electromagnética**		
5.1	Emisiones radiadas y susceptibilidad	Cumplimiento del Reglamento nº 10 de la CEPE.	218
5.2	Descarga electrostática	Cumplimiento de la norma ISO 10605: 2008 + Corrigendum Técnico 2010 + AMD1: 2014: +/– 4 kV para contacto +/– 8 kV para descarga de aire.	218
5.3	Susceptibilidad transitoria conducida en la fuente de alimentación	Para versiones 24 V: cumplimiento de la ISO 7637-2 + Reglamento nº 10 de la CEPE, Rev. 3: impulso 1a: Vs = – 450 V, Ri = 50 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 20 V, Ri = 0,05 ohmios impulso 3a: Vs = – 150 V, Ri = 50 ohmios impulso 3b: Vs = + 150 V, Ri = 50 ohmios impulso 4: Vs= – 16 V Va = – 12 V t6=100 ms impulso 5: Vs=+ 120 V Ri=2,2 ohmios td=250 ms. Para versiones 12 V: cumplimiento de la ISO 7637-1 + Reglamento nº 10 de la CEPE, Rev. 3: impulso 1: Vs = – 75 V, Ri = 10 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 10 V, Ri = 0,05 ohmios impulso 3a: Vs = – 112 V, Ri = 50 ohmios impulso 3b: Vs = + 75 V, Ri = 50 ohmios impulso 4: Vs= – 6 V Va= – 5 V t6=15 ms impulso 5: Vs= + 65 V Ri = 3 ohmios td = 100 ms. El impulso 5 deberá verificarse exclusivamente en las unidades intravehiculares concebidas para ser instaladas en vehículos que no dispongan de protección común externa contra volcado de la carga. Para las propuestas de volcado de la carga, remítase a la ISO 16750-2, 4ª edición, apartado 4.6.4.	218

3. PRUEBAS FUNCIONALES DEL SENSOR DE MOVIMIENTO

Nº	Prueba	Descripción	Condiciones correspondientes
1.	**Examen administrativo**		
1.1	Documentación	Corrección de la documentación.	

Nº	Prueba	Descripción	Condiciones correspondientes
2.	**Inspección visual**		
2.1.	Cumplimiento de lo dispuesto en la documentación		
2.2.	Identificación/inscripciones		225, 226
2.3	Materiales		219 a 223
2.4.	Precintos		398, 401 a 405
3.	**Pruebas funcionales**		
3.1	Datos de identificación del sensor		95 a 97*
3.2	Emparejamiento del sensor de movimiento y la unidad instalada en el vehículo		122*, 204
3.3	Detección de movimiento Precisión de la medición del movimiento.		30 a 35
3.4	Interfaz de la unidad instalada en el vehículo		02
3.5	Comprobar si el sensor de movimiento es invulnerable a los campos magnéticos constantes. De forma alternativa, comprobar si el sensor de movimiento reacciona a los campos magnéticos constantes perturbando la detección de movimiento del vehículo a fin de que la VU conectada pueda detectar, registrar y almacenar los fallos del sensor.		217
4.	**Pruebas ambientales**		
4.1	Temperatura de funcionamiento	Verificar la funcionalidad (tal y como se define en la prueba nº 3.3) en el intervalo de temperaturas [– 40 °C; + 135 °C] mediante: IEC 60068-2-1: prueba Ad, con una duración de 96 horas a la temperatura más baja $To_{mín}$. IEC 60068-2-2: prueba Bd, con una duración de 96 horas a la temperatura más alta $To_{máx}$. Prueba en virtud de la ISO 16750-4, sección 5.1.1.2: prueba de funcionamiento a temperatura baja (24 h a – 40 °C). Esta prueba se refiere a la IEC 60068-2-1: Verificación medioambiental — Parte 2-1: Pruebas — Prueba A: Frío. IEC 68-2-2: prueba Bd, con una duración de 96 horas a la temperatura más baja de – 40 °C. Prueba en virtud de la ISO 16750-4, apartado 5.1.2.2: prueba de funcionamiento a temperatura alta (96 h a 135 ° C). Esta prueba se refiere a la IEC 60068-2-2: Procedimientos básicos de verificación medioambiental; Parte 2: pruebas; Prueba B: Calor seco.	213

Nº	Prueba	Descripción	Condiciones correspondientes
4.2	Ciclos de temperatura	Prueba en virtud de la ISO 16750-4, apartado 5.3.2: cambio rápido de temperatura con una duración de transición específica (– 40 °C/135 °C, 20 ciclos, tiempo: 30 minutos en cada temperatura). IEC 60068-2-14: Verificación medioambiental — Parte 2-14: Pruebas — Prueba N: Variaciones de la temperatura.	213
4.3	Ciclos de humedad	Verificar la funcionalidad (tal y como se define en la prueba nº 3.3) mediante la IEC 60068-2-30, prueba Db, seis ciclos de 24 horas, con una variación de temperatura de + 25 °C a + 55 °C en cada caso y una humedad relativa del 97 % a + 25 °C y del 93 % a + 55 °C.	214
4.4	Vibración	ISO 16750-3: apartado 4.1.2.6: prueba VI: vehículo comercial, motor, caja de cambios. Prueba de vibración en modo combinado que incluya: a) una prueba de vibración sinusoidal, 20-520 Hz, 11,4-120 m/s^2, <= 0,5 oct/min; y b) una prueba de vibración aleatoria, 10-2 000 Hz, RMS 177 m/s^2 94 horas por eje, incluido un ciclo de temperatura de – 20 °C a 70 °C. Esta prueba se refiere a la IEC 60068-2-80: Verificación medioambiental — Parte 2-80: Pruebas — Prueba Fi: Vibración — Modo combinado	219
4.5	Choque mecánico	ISO 16750-3: apartado 4.2.3: prueba VI: prueba para los dispositivos situados en el interior o en la superficie de la caja de cambios. Choque semisinusoidal, aceleración acordada de entre 3 000 y 15 000 m/s^2, duración del impulso acordada, sin embargo (< 1 ms), número de choques acordados. Esta prueba se refiere a la IEC 60068-2-27: Verificación medioambiental — Parte 2: Pruebas. Prueba Ea y orientación: Choque.	219
4.6	Protección frente a la penetración de agua y cuerpos extraños	Prueba en virtud de la ISO 20653: Vehículos de carretera — Niveles de protección (código IP) — Protección del equipo eléctrico frente a objetos extraños, al agua y al acceso (valor objetivo IP 64).	220, 221
4.7	Protección frente a la inversión de la polaridad	Verificar que el sensor de movimiento es capaz de soportar una inversión de su fuente de alimentación.	216
4.8	Protección frente a cortocircuitos	Verificar que las señales de entrada y de salida están protegidas frente a cortocircuitos a la fuente de alimentación y a masa.	216

Nº	Prueba	Descripción	Condiciones correspondientes
5.	**Compatibilidad electromagnética**		
5.1	Emisiones radiadas y susceptibilidad	Verificar el cumplimiento del Reglamento nº 10 de la CEPE.	218
5.2	Descarga electrostática	Cumplimiento de la norma ISO 10605: 2008 + Corrigendum Técnico 2010 + AMD1: 2014: +/– 4 kV para contacto +/– 8 kV para descarga de aire.	218
5.3	Susceptibilidad transitoria conducida en las líneas de datos	Para versiones 24 V: cumplimiento de la ISO 7637-2 + Reglamento nº 10 de la CEPE, Rev. 3: impulso 1a: Vs = – 450 V, Ri = 50 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 20 V, Ri = 0,05 ohmios impulso 3a: Vs = – 150 V, Ri = 50 ohmios impulso 3b: Vs = + 150 V, Ri = 50 ohmios impulso 4: Vs= – 16 V Va= – 12 V t6 = 100 ms impulso 5: Vs=+120 V Ri=2,2 ohmios td=250 ms. Para versiones 12 V: cumplimiento de la ISO 7637-1 + Reglamento nº 10 de la CEPE, Rev. 3: impulso 1: Vs = – 75 V, Ri = 10 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 10 V, Ri = 0,05 ohmios impulso 3a: Vs = – 112 V, Ri = 50 ohmios impulso 3b: Vs = + 75 V, Ri = 50 ohmios impulso 4: Vs= – 6 V Va= – 5 V t6= 15 ms impulso 5: Vs= + 65 V Ri=3 ohmios td=100 ms. El impulso 5 deberá verificarse exclusivamente en las unidades intravehiculares concebidas para ser instaladas en vehículos que no dispongan de protección común externa contra volcado de la carga. Para las propuestas de volcado de la carga, remítase a la ISO 16750-2, 4ª edición, apartado 4.6.4.	218

4. PRUEBAS FUNCIONALES DE LAS TARJETAS DE TACÓGRAFO

Las pruebas previstas en el apartado 4,

nº 5 «Pruebas de protocolo»,

nº 6 «Estructura de la tarjeta» y

nº 7 «Pruebas funcionales»

puede llevarlas a cabo el evaluador o el certificador durante el proceso de certificación de la seguridad de los criterios comunes para el módulo del chip.

Las pruebas 2.3 y 4.2 son idénticas. Se trata de pruebas mecánicas para la combinación del cuerpo de la tarjeta con el módulo del chip. Deben realizarse estas pruebas cuando se modifique uno de estos componentes (cuerpo de la tarjeta o módulo del chip).

Nº	Prueba	Descripción	Condiciones correspondientes
1.	**Examen administrativo**		
1.1	Documentación	Corrección de la documentación.	
2	**Cuerpo de la tarjeta**		
2.1	Diseño impreso	Cerciorarse de que todas las características de protección y todos los datos visibles están bien impresos en la tarjeta y se ajustan a la normativa. [Designador] Anexo 1C, apartado 4.1 (datos visibles), 227 El anverso de la tarjeta contendrá: la mención «Tarjeta del conductor», «Tarjeta de control», «Tarjeta de taller» o «Tarjeta de empresa», en mayúsculas y en el o los idiomas oficiales del Estado miembro que expida la tarjeta, según el tipo de tarjeta. [Nombre del Estado miembro] Anexo 1C, apartado 4.1 (datos visibles), 228 El anverso de la tarjeta contendrá: el nombre del Estado miembro que expida la tarjeta (opcional). [Firma] Anexo 1C, apartado 4.1 (datos visibles), 229 El anverso de la tarjeta contendrá: el distintivo del Estado miembro que expida la tarjeta, impreso en negativo en un rectángulo azul rodeado de doce estrellas amarillas. [Numeración] Anexo 1C, apartado 4.1 (datos visibles), 232 El reverso de la tarjeta contendrá: una explicación de las rúbricas numeradas que aparecen en la primera página de la tarjeta. [Color] Anexo 1C, apartado 4.1 (datos visibles), 234 Las tarjetas de tacógrafo deberán imprimirse con los siguientes colores de fondo predominantes: — tarjeta del conductor: blanco, — tarjeta de taller: rojo, — tarjeta de control: azul, — tarjeta de empresa: amarillo.	227 a 229, 232, 234 a 236

Nº	Prueba	Descripción	Condiciones correspondientes
		[Seguridad] Anexo 1C, apartado 4.1 (datos visibles), 235 Las tarjetas de tacógrafo deberán reunir al menos las siguientes características de protección contra intentos de falsificación y manipulación: — un fondo con diseño de seguridad, fondo labrado e impresión en arco iris, — al menos una línea de microimpresión bicolor.	
		[Marcas] Anexo 1C, apartado 4.1 (datos visibles), 236 Los Estados miembros podrán añadir colores o marcas, como por ejemplo símbolos nacionales o características de seguridad.	
		[Marca de homologación] Las tarjetas de tacógrafo deberán incluir una marca de homologación. La marca de homologación estará compuesta por: — un rectángulo en el que se inscriba la letra «e» minúscula seguida de un número distintivo o de una letra distintiva del país que haya expedido una homologación; y — un número de homologación correspondiente al número de la ficha de homologación de la tarjeta del tacógrafo, colocado en cualquier posición cerca del rectángulo.	
2.2	Ensayos mecánicos	[Tamaño de la tarjeta] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [5] Dimensiones de la tarjeta [5.1] Tamaño de la tarjeta [5.1.1] Dimensiones y resistencia de la tarjeta Tipo de tarjeta ID-1: tarjeta no utilizada.	240, 243 ISO/IEC 7810
		[Bordes de la tarjeta] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [5] Dimensiones de la tarjeta [5.1] Tamaño de la tarjeta [5.1.2] Bordes de la tarjeta	

Nº	Prueba	Descripción	Condiciones correspondientes
		[Fabricación de la tarjeta] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [6] Fabricación de la tarjeta	
		[Materiales de la tarjeta] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [7] Materiales de la tarjeta	
		[Resistencia a la flexión] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.1] Resistencia a la flexión	
		[Toxicidad] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.3] Toxicidad	
		[Resistencia a los agentes químicos] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.4] Resistencia a los agentes químicos	
		[Estabilidad de la tarjeta] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.5] Estabilidad dimensional de la tarjeta y alabeado con la temperatura y la humedad	

Nº	Prueba	Descripción	Condiciones correspondientes
		[Ligera] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.6] Ligera	
		[Durabilidad] Anexo 1C, apartado 4.4 (especificaciones ambientales y eléctricas), 241 Las tarjetas de tacógrafo deberán poder funcionar correctamente durante cinco años si se utilizan con arreglo a las especificaciones ambientales y eléctricas.	
		[Resistencia de la superficie] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.8] Resistencia de la superficie	
		[Adherencia o bloqueo] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.9] Adherencia o bloqueo	
		[Alabeado] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.11] Alabeado general de la tarjeta	
		[Resistencia al calor] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.12] Resistencia al calor	

Nº	Prueba	Descripción	Condiciones correspondientes
		[Distorsiones de la superficie] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.13] Distorsiones de la superficie	
		[Contaminación] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810: Tarjetas de identificación — Características físicas: [8] Características de la tarjeta [8.14] Contaminación e interacción entre los componentes de la tarjeta	
2.3	Pruebas mecánicas con el módulo de chip integrado	[Flexión] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810:2003/Amd. 1:2009, Tarjetas de identificación — Características físicas, enmienda 1: criterios para las tarjetas que contienen circuitos integrados: [9.2] Tensión por flexión dinámica Nº total de ciclos de flexión: 4 000.	ISO/IEC 7810
		[Torsión] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810:2003/Amd. 1:2009, Tarjetas de identificación — Características físicas, enmienda 1: criterios para las tarjetas que contienen circuitos integrados: [9.3] Tensión por torsión dinámica Nº total de ciclos de torsión: 4 000.	
3	**Módulo**		
3.1	Módulo	El módulo está formado por el encapsulado del chip y el plato de contacto. [Perfil de la superficie] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7816-1:2011: Tarjetas de identificación — Tarjetas con circuitos integrados con contactos — Parte 1: Tarjetas con contactos — Características físicas: [4.2] Perfil de la superficie de los contactos	ISO/IEC 7816

Nº	Prueba	Descripción	Condiciones correspondientes
		[Resistencia mecánica] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7816-1:2011: Tarjetas de identificación — Tarjetas con circuitos integrados con contactos — Parte 1: Tarjetas con contactos — Características físicas: [4.3] Resistencia mecánica (de una tarjeta y de los contactos)	
		[Resistencia eléctrica] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7816-1:2011: Tarjetas de identificación — Tarjetas con circuitos integrados con contactos — Parte 1: Tarjetas con contactos — Características físicas: [4.4] Resistencia eléctrica (de los contactos)	
		[Dimensiones] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7816-2:2007: Tarjetas de identificación — Tarjetas con circuitos integrados con contactos — Parte 2: Tarjetas con contactos — Dimensiones y localización de los contactos: [3] Dimensiones de los contactos	
		[Localización] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7816-2:2007: Tarjetas de identificación — Tarjetas con circuitos integrados con contactos — Parte 2: Tarjetas con contactos — Dimensiones y localización de los contactos: [4] Número y localización de los contactos En caso de los módulos con seis contactos, los contactos C4 y C8 no están sujetos a este requisito.	
4	**Chip**		
4.1	Chip	[Temperatura de funcionamiento] El chip de la tarjeta de tacógrafo funcionará a una temperatura ambiente de entre –25 °C y +85 °C.	241 a 244 Reglamento nº 10 de la CEPE ISO/IEC 7810 ISO/IEC 10373

Nº	Prueba	Descripción	Condiciones correspondientes
		[Temperatura y humedad] Anexo 1C, apartado 4.4 (especificaciones ambientales y eléctricas), 241 Las tarjetas de tacógrafo deberán estar en condiciones de funcionar correctamente bajo cualquier condición climática habitual en el territorio de la Comunidad y al menos en el intervalo de temperaturas comprendido entre – 25 °C y + 70 °C, con picos ocasionales de hasta + 85 °C («ocasional» significa no más de 4 horas cada vez y no más de 100 veces durante la vida útil de la tarjeta). Las tarjetas de tacógrafo se exponen en fases consecutivas a las siguientes temperaturas y humedades durante un tiempo fijado. Se verifica la funcionalidad eléctrica de las tarjetas de tacógrafo después de cada una de las fases. 1. Temperatura de – 20 °C durante 2 horas. 2. Temperatura de +/– 0 °C durante 2 horas. 3. Temperatura de + 20 °C y humedad relativa del 50 % durante 2 horas. 4. Temperatura de + 50 °C y humedad relativa del 50 % durante 2 horas. 5. Temperatura de + 70 °C y humedad relativa del 50 % durante 2 horas. La temperatura se aumenta intermitentemente hasta + 85 °C, con una humedad relativa del 50 %, durante 60 min. 6. Temperatura de + 70 °C y humedad relativa del 85 %, durante 2 horas. La temperatura se aumenta intermitentemente hasta + 85 °C, con una humedad relativa del 85 %, durante 30 min.	
		[Humedad] Anexo 1C, apartado 4.4 (especificaciones ambientales y eléctricas), 242 Las tarjetas de tacógrafo deberán poder funcionar correctamente en el intervalo higrométrico comprendido entre el 10 % y el 90 %.	
		[Compatibilidad electromagnética (CEM)] Anexo 1C, apartado 4.4 (especificaciones ambientales y eléctricas), 244 Cuando se encuentren en funcionamiento, las tarjetas de tacógrafo deberán cumplir el Reglamento nº 10 de la CEPE en lo relativo a la compatibilidad electromagnética.	

Nº	Prueba	Descripción	Condiciones correspondientes
		[Electricidad estática] Anexo 1C, apartado 4.4 (especificaciones ambientales y eléctricas), 244 Cuando se encuentren en funcionamiento, las tarjetas de tacógrafo deberán estar protegidas contra descargas electroestáticas. Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810:2003/Amd. 1:2009: Tarjetas de identificación — Características físicas, enmienda 1: criterios para las tarjetas que contienen circuitos integrados: [9.4] Electricidad estática [9.4.1] Tarjetas de contacto IC Tensión de voltaje: 4 000 V	
		[Rayos X] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810:2003/Amd. 1:2009, Tarjetas de identificación — Características físicas, enmienda 1: criterios para las tarjetas que contienen circuitos integrados: [9.1] Rayos X	
		[Luz ultravioleta] ISO/IEC 10373-1:2006, Tarjetas de identificación — Métodos de prueba — Parte 1: Características generales [5.11] Luz ultravioleta	
		[3 ruedas] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 10373-1:2006/Amd. 1:2012, Tarjetas de identificación — Métodos de prueba — Parte 1: Características generales, Enmienda 1: [5.22] ICC — Resistencia mecánica: prueba de las tres ruedas para ICC con contactos	
		[Envoltura] Las tarjetas de tacógrafo deben ser conformes a la norma MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Prueba de la firmeza del envoltorio [13.2.1.32] TM-422: Fiabilidad mecánica: Prueba del envoltorio	

Nº	Prueba	Descripción	Condiciones correspondientes
4.2	Pruebas mecánicas del módulo del chip insertado en el cuerpo de la tarjeta –> ídem 2.3	[Flexión] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810:2003/Amd. 1:2009, Tarjetas de identificación — Características físicas, enmienda 1: criterios para las tarjetas que contienen circuitos integrados: [9.2] Tensión por flexión dinámica Nº total de ciclos de flexión: 4 000. [Torsión] Las tarjetas de tacógrafo deben ser conformes a la norma ISO/IEC 7810:2003/Amd. 1:2009, Tarjetas de identificación — Características físicas, enmienda 1: criterios para las tarjetas que contienen circuitos integrados: [9.3] Tensión por torsión dinámica Nº total de ciclos de torsión: 4 000.	ISO/IEC 7810
5	**Pruebas de protocolos**		
5.1	ATR	Comprobar si el ATR es conforme.	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Comprobar si el protocolo T=0 es conforme.	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Comprobar si el comando PTS es conforme. Para ello, ajustar T=1 partiendo de T=0.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Comprobar si el protocolo T=1 es conforme.	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Estructura de la tarjeta**		
6.1		Comprobar si la estructura de archivos de la tarjeta es conforme. Para ello, verificar la presencia de los archivos obligatorios en la tarjeta y sus condiciones de acceso.	TCS_22 a TCS_28 TCS_140 a TCS_179
7	**Pruebas funcionales**		
7.1	Proceso normal	Verificar al menos una vez por cada uso autorizado de cada comando (por ejemplo, verificar el comando UPDATE BINARY con CLA=00, CLA=0C y con diferentes parámetros P1, P2 y Lc). Comprobar que las operaciones se han llevado a cabo en la tarjeta (por ejemplo, leyendo el archivo donde se ha ejecutado el comando).	TCS_29 a TCS_139

Nº	Prueba	Descripción	Condiciones correspondientes
7.2	Mensajes de error	Comprobar al menos una vez cada uno de los mensajes de error (especificados en el apéndice 2) para cada comando. Comprobar al menos una vez cada uno de los errores genéricos (excepto los errores de integridad '**6400**' verificados durante la certificación de seguridad).	
7.3	Serie de cifrado y parámetros de dominio estandarizados		CSM_48, CSM_50
8	**Personalización**		
8.1	Personalización óptica	Anexo 1C, apartado 4.1 (datos visibles), 230 El anverso de la tarjeta contendrá: información específica de la tarjeta expedida. Anexo 1C, apartado 4.1 (datos visibles), 231 El anverso de la tarjeta contendrá: las fechas en formato «dd/mm/aaaa» o «dd.mm.aaaa» (día, mes, año). Anexo 1C, apartado 4.1 (datos visibles), 235 Las tarjetas de tacógrafo deberán reunir al menos las siguientes características de protección contra intentos de falsificación y manipulación: — en la zona de la fotografía, el fondo con diseño de seguridad y la fotografía deberán solaparse.	230, 231, 235

5. PRUEBAS DEL DISPOSITIVO GNSS EXTERNO

Nº	Prueba	Descripción	Condiciones correspondientes
1.	**Examen administrativo**		
1.1	Documentación	Corrección de la documentación.	
2.	**Inspección visual del dispositivo GNSS externo**		
2.1.	Cumplimiento de lo dispuesto en la documentación		
2.2.	Identificación/inscripciones		224 a 226
2.3	Materiales		219 a 223
3.	**Pruebas funcionales**		
3.1	Datos de identificación del sensor		98, 99
3.2	Acoplamiento entre el módulo GNSS externo y la unidad instalada en el vehículo		123, 205

Nº	Prueba	Descripción	Condiciones correspondientes
3.3	Posición GNSS		36, 37
3.4	Interfaz de la unidad instalada en el vehículo cuando el receptor GNSS es externo a la unidad		03
3.5	Serie de cifrado y parámetros de dominio estandarizados		CSM_48, CSM_50
4.	**Pruebas ambientales**		
4.1	Temperatura	Verificar la funcionalidad mediante: Prueba en virtud de la ISO 16750-4, apartado 5.1.1.2: prueba de funcionamiento a temperatura baja (72 h a −20 ° C). Esta prueba se refiere a la IEC 60068-2-1: Verificación medioambiental — Parte 2-1: Pruebas — Prueba A: Frío Prueba en virtud de la ISO 16750-4, apartado 5.1.2.2: prueba de funcionamiento a temperatura alta (72 h a 70 ° C). Esta prueba se refiere a la IEC 60068-2-2: Procedimientos básicos de verificación medioambiental; Parte 2: pruebas; Prueba B: Calor seco. Prueba en virtud de la ISO 16750-4, apartado 5.3.2: cambio rápido de temperatura con una duración de transición específica (– 20 °C/70 °C, 20 ciclos, tiempo: 1 hora en cada temperatura). Es posible llevar a cabo un conjunto reducido de pruebas (de entre las que se definen en la sección 3 de esta tabla) a la temperatura más baja, a la temperatura más alta y durante los ciclos de temperatura.	213
4.2	Humedad	Verificar que la unidad instalada en el vehículo puede soportar una humedad cíclica (prueba de calor) mediante IEC 60068-2-30, prueba Db, seis ciclos de 24 horas, con una variación de temperatura de + 25 °C a + 55 °C en cada caso y una humedad relativa del 97 % a + 25°C y del 93 % a + 55°C.	214
4.3	Mecánica	1. Vibraciones sinusoidales: verificar que la unidad instalada en el vehículo es capaz de soportar vibraciones sinusoidales de las siguientes características: desplazamiento constante entre 5 y 11 Hz: pico de 10 mm; y aceleración constante entre 11 y 300 Hz: 5 g. Esta exigencia se verifica mediante la norma IEC 60068-2-6, prueba Fc, con una duración mínima de 3 × 12 horas (12 horas por cada eje). La ISO 16750-3 no requiere una prueba de vibración sinusoidal para dispositivos situados en el puesto de conducción del vehículo desacoplado.	219

Nº	Prueba	Descripción	Condiciones correspondientes
		2. Vibraciones aleatorias: Prueba en virtud de la ISO 16750-3, apartado 4.1.2.8: prueba VIII: vehículo comercial, puesto de conducción del vehículo desacoplado. Prueba de vibraciones aleatorias, 10-2 000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 3 ejes, 32 horas por eje, incluido un ciclo de temperatura – 20-+ 70 °C. Esta prueba se refiere a la IEC 60068-2-64: Verificación medioambiental — Parte 2-64: Pruebas — Prueba Fh: Vibración, aleatorio de banda ancha y orientación. 3. Choques: choque mecánico con semionda sinusoidal de 3 g de conformidad con la ISO 16750. Las pruebas arriba descritas se llevan a cabo con muestras diferentes del tipo de equipo que se someta a prueba.	
4.4	Protección frente a la penetración de agua y cuerpos extraños	Prueba en virtud de la ISO 20653: Vehículos de carretera — Niveles de protección (código IP) — Protección del equipo eléctrico frente a objetos extraños, al agua y al acceso (sin cambio en los parámetros).	220, 221
4.5	Protección frente a sobretensiones	Verificar que la unidad instalada en el vehículo es capaz de soportar un suministro eléctrico de: versiones de 24 V: 34 V a + 40 °C 1 hora. versiones de 12 V: 17 V a + 40 °C 1 hora. (ISO 16750-2, apartado 4.3)	216
4.6	Protección frente a la inversión de la polaridad	Verificar que la unidad instalada en el vehículo es capaz de soportar una inversión de su fuente de alimentación. (ISO 16750-2, apartado 4.7)	216
4.7	Protección frente a cortocircuitos	Verificar que las señales de entrada y de salida están protegidas frente a cortocircuitos a la fuente de alimentación y a masa. (ISO 16750-2, apartado 4.10)	216
5	**Pruebas de compatibilidad electromagnética**		
5.1	Emisiones radiadas y susceptibilidad	Cumplimiento del Reglamento nº 10 de la CEPE.	218

Nº	Prueba	Descripción	Condiciones correspondientes
5.2	Descarga electrostática	Cumplimiento de la norma ISO 10605: 2008 + Corrigendum Técnico 2010 + AMD1: 2014: +/– 4 kV para contacto +/– 8 kV para descarga de aire.	218
5.3	Susceptibilidad transitoria conducida en la fuente de alimentación	Para versiones 24 V: cumplimiento de la ISO 7637-2 + Reglamento nº 10 de la CEPE, Rev. 3: impulso 1a: Vs = – 450 V, Ri = 50 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 20 V, Ri = 0,05 ohmios impulso 3a: Vs = – 150 V, Ri = 50 ohmios impulso 3b: Vs = + 150 V, Ri = 50 ohmios impulso 4: Vs= – 16 V Va=–12 V t6=100 ms impulso 5: Vs=+ 120 V Ri=2,2 ohmios td=250 ms. Para versiones 12 V: cumplimiento de la ISO 7637-1 + Reglamento nº 10 de la CEPE, Rev. 3: impulso 1: Vs = – 75 V, Ri = 10 ohmios impulso 2a: Vs = + 37 V, Ri = 2 ohmios impulso 2b: Vs = + 10 V, Ri = 0,05 ohmios impulso 3a: Vs = – 112 V, Ri = 50 ohmios impulso 3b: Vs = + 75 V, Ri = 50 ohmios impulso 4: Vs= – 6 V Va=–5 V t6=15 ms impulso 5: Vs= + 65 V Ri=3 ohmios td=100 ms. El impulso 5 deberá verificarse exclusivamente en las unidades intravehiculares concebidas para ser instaladas en vehículos que no dispongan de protección común externa contra volcado de la carga. Para las propuestas de volcado de la carga, remítase a la ISO 16750-2, 4ª edición, apartado 4.6.4.	218

6. PRUEBAS DE LA INSTALACIÓN DE COMUNICACIÓN REMOTA

Nº	Prueba	Descripción	Condiciones correspondientes
1.	**Examen administrativo**		
1.1	Documentación	Corrección de la documentación.	
2.	**Inspección visual**		
2.1.	Cumplimiento de lo dispuesto en la documentación		
2.2.	Identificación/inscripciones		225, 226
2.3	Materiales		219 a 223

Nº	Prueba	Descripción	Condiciones correspondientes
4.	**Pruebas ambientales**		
4.1	Temperatura	Verificar la funcionalidad mediante: Prueba en virtud de la ISO 16750-4, apartado 5.1.1.2: prueba de funcionamiento a temperatura baja (72 h a – 20 °C). Esta prueba se refiere a la IEC 60068-2-1: Verificación medioambiental — Parte 2-1: Pruebas — Prueba A: Frío. Prueba en virtud de la ISO 16750-4, apartado 5.1.2.2: prueba de funcionamiento a temperatura alta (72 h a 70 ° C). Esta prueba se refiere a la IEC 60068-2-2: Procedimientos básicos de verificación medioambiental; Parte 2: pruebas; Prueba B: Calor seco. Prueba en virtud de la ISO 16750-4, apartado 5.3.2: cambio rápido de temperatura con una duración de transición específica (– 20°C/70 °C, 20 ciclos, tiempo: 1 hora (?) en cada temperatura). Es posible llevar a cabo un conjunto reducido de pruebas (de entre las que se definen en la sección 3 de esta tabla) a la temperatura más baja, a la temperatura más alta y durante los ciclos de temperatura.	213
4.4	Protección frente a la penetración de agua y cuerpos extraños	Prueba en virtud de la ISO 20653: Vehículos de carretera — Niveles de protección (código IP) — Protección del equipo eléctrico frente a objetos extraños, al agua y al acceso (valor objetivo IP40)	220, 221
5	**Pruebas de compatibilidad electromagnética**		
5.1	Emisiones radiadas y susceptibilidad	Cumplimiento del Reglamento nº 10 de la CEPE.	218
5.2	Descarga electrostática	Cumplimiento de la norma ISO 10605: 2008 + Corrigendum Técnico 2010 + AMD1: 2014: +/– 4 kV para contacto +/– 8 kV para descarga de aire.	218
5.3	Susceptibilidad transitoria conducida en la fuente de alimentación	Para versiones 24 V: cumplimiento de la ISO 7637-2 + Reglamento nº 10 de la CEPE, Rev. 3: impulso 1a: Vs = –450 V, Ri = 50 ohmios impulso 2a: Vs = +37 V, Ri = 2 ohmios impulso 2b: Vs = +20 V, Ri = 0,05 ohmios impulso 3a: Vs = –150 V, Ri = 50 ohmios impulso 3b: Vs = +150 V, Ri = 50 ohmios impulso 4: Vs= –16 V Va=–12 V t6=100 ms impulso 5: Vs=+120 V Ri=2,2 ohmios td=250 ms.	218

Nº	Prueba	Descripción	Condiciones correspondientes
		Para versiones 12 V: cumplimiento de la ISO 7637-1 + Reglamento nº 10 de la CEPE, Rev. 3: impulso 1: Vs = –75 V, Ri = 10 ohmios impulso 2a: Vs = +37 V, Ri = 2 ohmios impulso 2b: Vs = +10 V, Ri = 0,05 ohmios impulso 3a: Vs = –112 V, Ri = 50 ohmios impulso 3b: Vs = +75 V, Ri = 50 ohmios impulso 4: Vs= – 6 V Va= – 5 V t6=15 ms impulso 5: Vs= + 65 V Ri=3 ohmios td=100 ms. El impulso 5 deberá verificarse exclusivamente en las unidades intravehiculares concebidas para ser instaladas en vehículos que no dispongan de protección común externa contra volcado de la carga. Para las propuestas de volcado de la carga, remítase a la ISO 16750-2, 4ª edición, apartado 4.6.4.	

7. PRUEBAS FUNCIONALES DEL PAPEL

Nº	Prueba	Descripción	Condiciones correspondientes
1.	**Examen administrativo**		
1.1	Documentación	Corrección de la documentación.	
2	**Pruebas generales**		
2.1	Número de caracteres por línea	Inspección visual de los documentos de impresión.	172
2.2	Tamaño mínimo de los caracteres	Inspección visual de los documentos de impresión e inspección de los caracteres.	173
2.3	Conjuntos de caracteres admitidos	La impresora admitirá el uso de los caracteres especificados en el apéndice 1, apartado 4 (Conjuntos de caracteres).	174
2.4	Definición de los documentos de impresión	Verificación de la homologación del tacógrafo e inspección visual de los documentos de impresión.	174
2.5	Legibilidad e identificación de los documentos de impresión	Inspección de los documentos de impresión. Demostración mediante los informes de prueba y los protocolos de verificación del fabricante. Todos los números de homologación de los tacógrafos con los que se pueda emplear la impresora están impresos en el papel.	175, 177, 178
2.6	Inclusión de notas escritas a mano	Inspección visual: Existencia de un espacio para la firma del conductor. Existencia de espacios para la inclusión de otros textos escritos a mano.	180

Nº	Prueba	Descripción	Condiciones correspondientes
2.7	Detalles adicionales en el papel	Tanto el anverso como el reverso del papel pueden incluir detalles o información adicionales. Estos últimos no podrán alterar la legibilidad de los documentos de impresión. Inspección visual.	177, 178
3	**Pruebas de almacenamiento**		
3.1	Calor seco	Preacondicionamiento: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 % Prueba ambiental: 72 horas a +70 °C ±2 °C Recuperación: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 %	176, 178 IEC 60068-2-2-Bb
2.2	Calor húmedo	Preacondicionamiento: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 % Prueba ambiental: 144 horas a +55 °C ±2 °C/humedad relativa del 93 % ±3 % Recuperación: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 %	176, 178 IEC 60068-2-78-Cab
4	**Pruebas del papel durante el servicio**		
4.1	Resistencia a la humedad del fondo (papel no impreso)	Preacondicionamiento: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 % Prueba ambiental: 144 horas a +55 °C ±2 °C/humedad relativa del 93 % ±3 % Recuperación: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 %	176, 178 IEC 60068-2-78-Cab
4.2	Imprimabilidad	Preacondicionamiento: 24 horas a +40 °C ±2 °C/humedad relativa del 93 % ± 3 % Prueba ambiental: documento de impresión realizado a +23 °C ± 2 °C Recuperación: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 %	176, 178
4.3	Resistencia al calor	Preacondicionamiento: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 % Prueba ambiental: 2 horas a +70 °C ±2 °C/calor seco Recuperación: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 %	176, 178 IEC 60068-2-2-Bb
4.4	Resistencia a temperaturas bajas	Preacondicionamiento: 16 horas a +23 °C ± 2 °C/humedad relativa del 55 % ±3 % Prueba ambiental: 24 horas a +20 °C ±3 °C/frío seco Recuperación: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 %	176, 178 ISO 60068-2-1-Ab

Nº	Prueba	Descripción	Condiciones correspondientes
4.5	Resistencia a la luz	Preacondicionamiento: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 % Prueba ambiental: 100 horas con una iluminación inferior a 5 000 lux a +23 °C ±2 °C/humedad relativa del 55 % ±3 % Recuperación: 16 horas a +23 °C ±2 °C/humedad relativa del 55 % ±3 %	176, 178

Criterios de legibilidad para las pruebas 3.x y 4.x:

Queda garantizada la legibilidad de los documentos de impresión si las densidades ópticas respetan los siguientes límites:

Caracteres impresos: mín. 1,0

Fondo (papel no impreso): máx. 0,2

Las densidades ópticas de los documentos de impresión resultantes deben medirse en función de la norma DIN EN ISO 534.

Los documentos de impresión no deberán sufrir cambios dimensionales y deberán mantener una legibilidad clara.

8. PRUEBAS DE INTEROPERABILIDAD

Nº	Prueba	Descripción
	9.1 Pruebas de interoperabilidad entre las unidades intravehiculares y las tarjetas de tacógrafo	
1	Autenticación mutua	Comprobar que la autenticación mutua entre la unidad instalada en el vehículo y la tarjeta de tacógrafo funciona normalmente.
2	Pruebas de lectura/escritura	Ejecutar un escenario de actividad típico en la unidad instalada en el vehículo. Dicho escenario deberá adaptarse al tipo de tarjeta que se esté verificando y deberá incluir pruebas de escritura en tantos EF como sea posible en la tarjeta. Verificar mediante una transferencia de la unidad instalada en el vehículo que todos los registros correspondientes se han realizado correctamente. Verificar mediante una transferencia de la tarjeta que todos los registros correspondientes se han realizado correctamente. Verificar mediante una impresión diaria que todos los registros correspondientes se pueden leer correctamente.
	9.2 Pruebas de interoperabilidad entre las unidades intravehiculares y los sensores de movimiento	
1	Emparejamiento	Comprobar que el emparejamiento entre las unidades intravehiculares y los sensores de movimiento funciona normalmente.
2	Pruebas de actividad	Ejecutar un escenario de actividad típico en el sensor de movimiento. El escenario incluirá una actividad normal y creará el mayor número de incidentes o fallos posible. Verificar mediante una transferencia de la unidad instalada en el vehículo que todos los registros correspondientes se han realizado correctamente. Verificar mediante una transferencia de la tarjeta que todos los registros correspondientes se han realizado correctamente. Verificar mediante una impresión diaria que todos los registros correspondientes se pueden leer correctamente.

Nº	Prueba	Descripción
9.3 Pruebas de interoperabilidad entre las unidades intravehiculares y las instalaciones GNSS externas (si procede)		
1	Autenticación mutua	Comprobar que la autenticación mutua (acoplamiento) entre la unidad instalada en el vehículo y el módulo GNSS externo funciona normalmente.
2	Pruebas de actividad	Ejecutar un escenario de actividad típico en el módulo GNSS externo. El escenario incluirá una actividad normal y creará el mayor número de incidentes o fallos posible. Verificar mediante una transferencia de la unidad instalada en el vehículo que todos los registros correspondientes se han realizado correctamente. Verificar mediante una transferencia de la tarjeta que todos los registros correspondientes se han realizado correctamente. Verificar mediante una impresión diaria que todos los registros correspondientes se pueden leer correctamente.

Apéndice 10

REQUISITOS DE SEGURIDAD

En el presente apéndice se especifican los requisitos en materia de seguridad informática para los componentes del sistema de tacógrafo inteligente (tacógrafo de segunda generación).

SEC_001 Los componentes del sistema de tacógrafo inteligente que se recogen a continuación deberán tener una certificación de seguridad conforme con el sistema de criterios comunes:

— unidad instalada en el vehículo,

— tarjeta de tacógrafo,

— sensor de movimiento,

— Dispositivo GNSS externo

SEC_002 Los requisitos mínimos de seguridad informática que debe cumplir cada componente con certificación de seguridad se determinarán en un Perfil de Protección de los componentes de acuerdo con el sistema de criterios comunes.

SEC_003 La Comisión Europea se asegurará de que se patrocinen, elaboren y aprueben por los organismos de certificación de la seguridad informática nacionales, en el marco del Grupo de Trabajo de interpretación conjunta, que es el grupo de trabajo que apoya el reconocimiento mutuo de certificados en el contexto del acuerdo europeo SOGIS-MRA (Acuerdo sobre el reconocimiento mutuo de los certificados de evaluación de la seguridad de la tecnología de la información), cuatro perfiles de protección conformes con el presente anexo:

— Perfil de Protección para la unidad instalada en el vehículo,

— Perfil de Protección para la tarjeta de tacógrafo,

— Perfil de Protección para el sensor de movimiento,

— Perfil de protección para el dispositivo GNSS externo.

El perfil de protección para la unidad instalada en el vehículo debe abordar los casos en que la VU está diseñada para ser utilizada con un dispositivo GNSS externo o sin él. En el primer caso los requisitos de seguridad del dispositivo GNSS externo son los recogidos en el Perfil de Protección específico.

SEC_004 Los fabricantes deberán perfeccionar y completar, en la medida de lo necesario, el Perfil de Protección de los componentes sin borrar o modificar especificaciones en materia de amenazas, objetivos, procedimientos y funciones de aplicación de las normas de seguridad con el fin de establecer un objetivo de seguridad conforme al cual se exigirá la certificación de seguridad del componente.

SEC_005 En el proceso de evaluación se comprobará de forma estricta la conformidad del objetivo de seguridad específico con el correspondiente Perfil de Protección.

SEC_006 El nivel de garantía de cada Perfil de Protección será EAL4 incrementado por los componentes de garantía ATE_DPT.2 y AVA_VAN.5.

Apéndice 11

MECANISMOS COMUNES DE SEGURIDAD

ÍNDICE

PREÁMBULO

El presente apéndice especifica los mecanismos de seguridad que garantizan

— la autenticación mutua entre los diferentes componentes del sistema de tacógrafo digital;

— la confidencialidad, integridad, autenticidad y/o no rechazo de los datos transferidos entre equipos diferentes o descargados a medios de almacenamiento externos.

El presente apéndice consta de dos partes. La Parte A define los mecanismos de seguridad del sistema de tacógrafo de primera generación (tacógrafo digital). La Parte A define los mecanismos de seguridad del sistema de tacógrafo de segunda generación (tacógrafo inteligente).

Los mecanismos especificados en la Parte A del presente apéndice serán de aplicación si al menos uno de los componentes del sistema de tacógrafo implicados en una autenticación mutua y/o proceso de transferencia de datos es de primera generación.

Los mecanismos especificados en la Parte B del presente apéndice serán de aplicación si los dos componentes del sistema de tacógrafo implicados en la autenticación mutua y/o el proceso de transferencia de datos son de segunda generación.

El apéndice 15 contiene más información sobre el uso de componentes de primera generación en combinación con componentes de segunda generación.

PARTE A

SISTEMA DE TACÓGRAFO DE PRIMERA GENERACIÓN

1. INTRODUCCIÓN

1.1. **Referencias**

En el presente apéndice aparecen las siguientes referencias:

SHA-1	National Institute of Standards and Technology (NIST). *Publicación FIPS 180-1:* Norma sobre códigos de comprobación seguros. Abril de 1995.
PKCS1	RSA Laboratories. PKCS # 1: Norma de cifrado RSA. Versión 2.0. Octubre de 1998.
TDES	National Institute of Standards and Technology (NIST). *Publicación FIPS 46-3:* Norma de cifrado de datos. Proyecto de 1999.
TDES-OP	ANSI X9.52, Modos de funcionamiento del algoritmo triple de cifrado de datos. 1998.
ISO/IEC 7816-4	Tecnologías de la Información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 4: Comandos interindustriales para intercambio. Primera edición: 1995 + Modificación 1: 1997.
ISO/IEC 7816-6	Tecnologías de la Información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 6: Elementos de datos interindustriales. Primera edición: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Tecnologías de la Información — Tarjetas de identificación — Tarjetas de circuito(s) integrado(s) con contactos — Parte 8: Comandos interindustriales relacionados con la seguridad. Primera edición 1999.
ISO/IEC 9796-2	Tecnología de la información — Técnicas de seguridad — Esquemas de firma digital con recuperación de mensaje — Parte 2: Mecanismos que emplean una función de comprobación aleatoria. Primera edición: 1997.
ISO/IEC 9798-3	Tecnología de la información — Técnicas de seguridad — Mecanismos de autenticación de entidades — Parte 3: autenticación de entidades mediante un algoritmo de clave pública. Segunda edición 1998.
ISO 16844-3	Vehículos de carretera — Sistemas de tacógrafo — Parte 3: Interfaz del sensor de movimiento.

1.2. **Notaciones y términos abreviados**

En el presente apéndice se emplean las siguientes notaciones y términos abreviados:

(K_a, K_b, K_c)	Un conjunto de claves que utiliza el algoritmo triple de cifrado de datos.
CA	Certification authority (/autoridad de certificación),
CAR	Certification authority reference (/referencia a la autoridad de certificación),
CC	Cryptographic checksum (/suma de control criptográfica),
CG	Criptograma,
CH	Command header (/cabecera de comando),
CHA	Certificate holder authorisation (/autorización del titular del certificado),
CHR	Certificate holder reference (/referencia al titular del certificado),
D()	Descifrado con DES,

DE	Data element (/elemento de datos),
DO	Data object (/objeto de datos),
d	Clave privada RSA, exponente privado,
e	Clave pública RSA, exponente público,
E()	Cifrado con DES,
EQT	EQT Equipment (/equipo),
Hash()	Valor de comprobación aleatoria, una salida de Hash,
Hash	Función de comprobación aleatoria,
KID	Key identifier (/identificador de clave),
Km	Clave TDES. Clave maestra definida en ISO 16844-3,
Km_{VU}	Clave TDES insertada en las unidades de vehículos,
Km_{WC}	Clave TDES insertada en las tarjetas de los centros de ensayo,
m	Representante de mensaje, un número entero entre 0 y n-1,
n	Claves RSA, módulo,
PB	Padding bytes (/bytes de relleno),
PI	Padding indicator byte (/byte indicador de relleno, se utiliza en un criptograma para confidencialidad DO),
PV	Plain value (/valor sencillo),
s	Representante de la firma, un número entero entre 0 y n-1,
SSC	Send sequence counter (/contador de la secuencia de envío),
SM	Secure messaging (/mensajería segura),
TCBC	Modo de funcionamiento por cifrado progresivo TDEA,
TDEA	Algoritmo triple de cifrado de datos,
TLV	Tag length value (/valor de longitud de la etiqueta),
VU	Vehicle unit (/unidad instalada en el vehículo),
X.C	Certificado del usuario X, expedido por una autoridad de certificación,
X.CA	Una autoridad de certificación del usuario X,
X.CA.PK $_{o}$ X.C	La operación de abrir un certificado para extraer una clave pública. Se trata de un operador infijo, cuyo operando izquierdo es la clave pública de una autoridad de certificación, y cuyo operando derecho es el certificado expedido por dicha autoridad. El resultado es la clave pública del usuario X cuyo certificado es el operando derecho,
X.PK	Clave pública RDS de un usuario X,
X.PK[I]	Cifrado RSA de cierta información I, utilizando la clave pública del usuario X,
X.SK	Clave privada RDS de un usuario X,
X.SK[I]	Cifrado RSA de cierta información I, utilizando la clave privada del usuario X,
'xx'	Un valor hexadecimal,
||	Operador de concatenación.

2. SISTEMAS Y ALGORITMOS CRIPTOGRÁFICOS

2.1. **Sistemas criptográficos**

CSM_001 Las unidades instaladas en los vehículos y las tarjetas de tacógrafo deberán emplear un sistema criptográfico RSA clásico de clave pública para ofrecer los siguientes mecanismos de seguridad:

— autenticación entre unidades instaladas en los vehículos y tarjetas,

— transporte de claves de sesión triple DES entre las unidades instaladas en los vehículos y las tarjetas de tacógrafo,

— firma digital de los datos transferidos desde unidades instaladas en los vehículos o tarjetas de tacógrafo a medios externos.

CSM_002 Las unidades instaladas en los vehículos y las tarjetas de tacógrafo deberán emplear un sistema criptográfico simétrico triple DES para ofrecer un mecanismo que garantice la integridad de los datos durante los intercambios de datos de usuario entre las unidades instaladas en los vehículos y las tarjetas de tacógrafo, y para ofrecer, cuando proceda, la confidencialidad en los intercambios de datos entre las unidades instaladas en los vehículos y las tarjetas de tacógrafo.

2.2. **Algoritmos criptográficos**

2.2.1 *Algoritmo RSA*

CSM_003 El algoritmo RSA se define íntegramente con las relaciones siguientes:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

En el documento de referencia PKCS1 figura una descripción más completa de la función RSA. El exponente público e será, para los cálculos RSA, un entero comprendido entre 3 y n-1, cumpliéndose que mcd(e, mcm(p-1, q-1))=1.

2.2.2 *Algoritmo de comprobación aleatoria*

CSM_004 Los mecanismos de firma digital deberán emplear el algoritmo SHA-1 de comprobación aleatoria, que se define en el documento de referencia SHA-1.

2.2.3 *Algoritmo de cifrado de datos*

CSM_005 En el modo de funcionamiento por cifrado progresivo deberán emplearse algoritmos con base DES.

3. CLAVES Y CERTIFICADOS

3.1. **Generación y distribución de claves**

3.1.1 *Generación y distribución de claves RSA*

CSM_006 Las claves RSA deberán generarse en tres niveles jerárquicos funcionales:

— Nivel europeo

— Nivel de Estado miembro

— Nivel de equipo

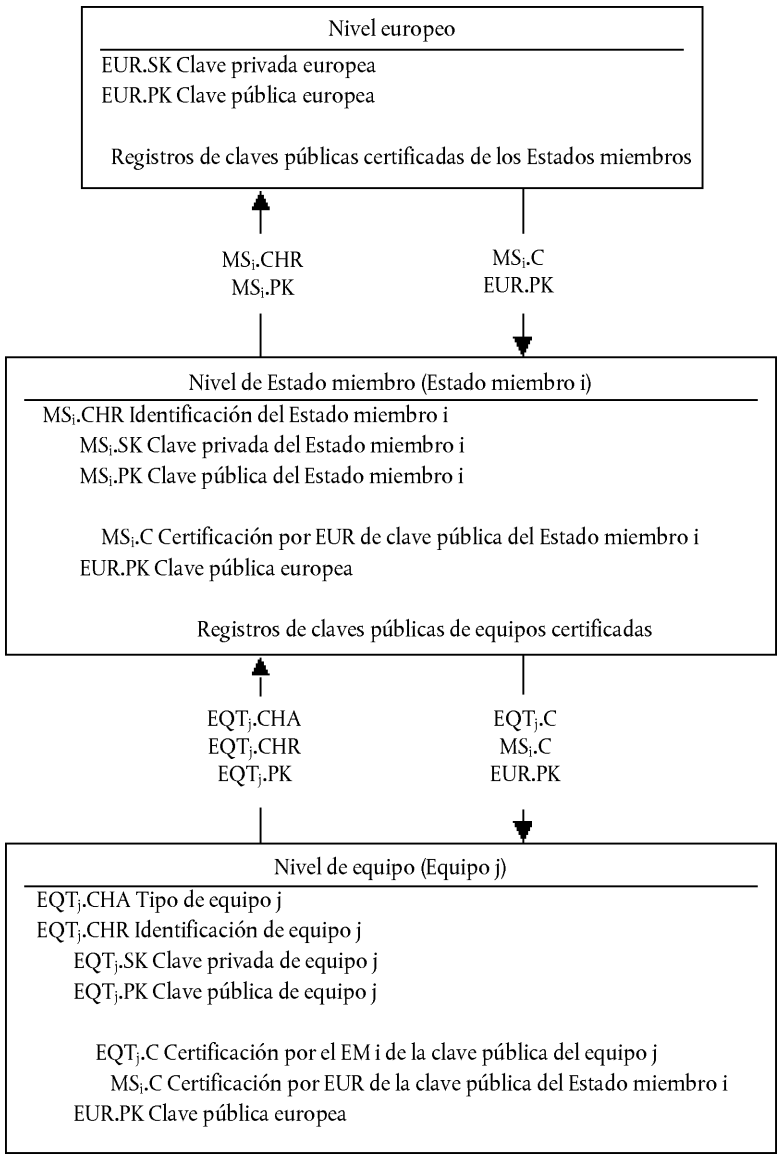
CSM_007 En el nivel europeo deberá generarse un único par de claves europeas (EUR.SK y EUR.PK). La clave privada europea deberá emplearse para certificar las claves públicas de los Estados miembros. Se conservarán registros de todas las claves certificadas. Todas estas tareas se realizarán bajo la gestión de una autoridad de certificación europea, y bajo la autoridad y la responsabilidad de la Comisión Europea.

CSM_008 En el nivel de los Estados miembros, deberá generarse un par de claves de Estado miembro (MS.SK y MS.PK). La autoridad de certificación europea se encargará de certificar las claves públicas de los Estados miembros. La clave privada del Estado miembro deberá emplearse para certificar las claves públicas que vayan a introducirse en el equipo (unidad instalada en el vehículo o tarjeta de tacógrafo). Se conservarán registros de todas las claves públicas certificadas, junto con la identificación del equipo al que están destinadas. Estas tareas serán efectuadas por una autoridad de certificación del Estado miembro que corresponda. Un Estado miembro podrá cambiar periódicamente su par de claves.

CSM_009 En el nivel de equipo, deberá generarse e introducirse en cada equipo un único par de claves (EQT.SK y EQT.PK). Estas tareas serán gestionadas por una autoridad de certificación del Estado miembro que corresponda. Estas tareas podrán ser efectuadas por los fabricantes de los equipos, los personalizadores de los equipos o las autoridades de los Estados miembros. Este par de claves se emplea para los servicios de autenticación, firma digital y cifrado.

CSM_010 Se deberá mantener la confidencialidad de las claves privadas durante su generación, transporte (en su caso) y almacenamiento.

El gráfico siguiente resume el flujo de datos en este proceso:



3.1.2 *Claves de prueba RSA*

CSM_011 Con el fin de verificar los equipos (incluidas las pruebas de interoperabilidad), la autoridad de certificación europea deberá generar otro par de claves de prueba europeas y al menos dos pares de claves de prueba de Estado miembro, cuyas claves públicas deberán certificarse con la clave privada de prueba europea. Los fabricantes deberán introducir, en el equipo que se someta a las pruebas de homologación, las claves de prueba certificadas por una de estas claves de prueba de Estado miembro.

3.1.3 *Claves del sensor de movimiento*

La confidencialidad de las tres claves TDES descritas a continuación se mantendrá adecuadamente durante la generación, el transporte (si lo hay) y el almacenamiento.

A fin de admitir componentes de tacógrafo conformes con la norma ISO 16844, la autoridad de certificación europea y las autoridades de certificación de los Estados miembros garantizarán, además, lo siguiente:

CSM_036 La autoridad de certificación europea generará KmVU y KmWC, dos claves Triple DES independientes y únicas, y generará Km como: $Km = Km_{VU}$ XOR Km_{WC}. La autoridad de certificación europea remitirá estas claves, con arreglo a procedimientos de seguridad adecuados, a las autoridades de certificación de los Estados miembros a petición de éstas.

CSM_037 Las autoridades de certificación europeas:

— utilizarán Km para cifrar los datos del sensor de movimiento solicitados por los fabricantes del sensor de movimiento (los datos que deben cifrarse con Km se definen en ISO 16844-3),

— remitirán Km_{VU} a los fabricantes de la unidad instalada en el vehículo, con arreglo a procedimientos de seguridad adecuados, para su inserción en las unidades del vehículo,

— se encargarán de que Km_{WC} se inserte en todas las tarjetas de centros de ensayo (`SensorInstallationSecData` en el archivo elemental `Sensor_Installation_Data`) durante la personalización de la tarjeta.

3.1.4 *Generación y distribución de claves de sesión T-DES*

CSM_012 Las unidades instaladas en los vehículos y las tarjetas de tacógrafo deberán, como parte del proceso de autenticación mutua, generar e intercambiar los datos necesarios para elaborar una clave común de sesión triple DES. La confidencialidad de este intercambio de datos deberá estar protegida por un mecanismo criptográfico RSA.

CSM_013 Esta clave deberá emplearse en todas las operaciones criptográficas subsiguientes que utilicen mensajería segura. Su validez expirará al término de cada sesión (al retirar o restaurar la tarjeta) o después de 240 usos (un uso de la clave = un comando que se envíe a la tarjeta y utilice mensajería segura, y la respuesta asociada).

3.2. **Claves**

CSM_014 Las claves RSA (con independencia de su nivel) deberán tener las longitudes siguientes: módulo *n* 1 024 bits, exponente público *e* 64 bits máximo, exponente privado *d* 1 024 bits.

CSM_015 Las claves triple DES deberán tener la forma (K_a, K_b, K_a), donde K_a y K_b son claves independientes con una longitud de 64 bits. No se configurarán bits para la detección de errores de paridad.

3.3. **Certificados**

CSM_016 Los certificados de clave pública RSA deberán ser «no autodescriptivos» y «verificables con tarjeta» (ref.: ISO/IEC 7816-8).

3.3.1 *Contenido de los certificados*

CSM_017 Los certificados de clave pública RSA incluyen los datos siguientes en este orden:

Dato	Formato	Bytes	Obs
CPI	Nº ENTERO	1	Identificador de perfil del certificado ('01' para esta versión)
CAR	CADENA DE OCTETOS	8	Referencia a la autoridad de certificación
CHA	CADENA DE OCTETOS	7	Autorización del titular del certificado
EOV	Fecha	4	Fin de la validez del certificado. Este dato es opcional y se rellena con las letras 'FF' si no se utiliza.
CHR	CADENA DE OCTETOS	8	Referencia al titular del certificado
n	CADENA DE OCTETOS	128	Clave pública (módulo)
e	CADENA DE OCTETOS	8	Clave pública (exponente público)
		164	

Notas:

1. El «Identificador de perfil del certificado» (CPI) define la estructura exacta de un certificado de autenticación. Se puede utilizar como un identificador interno del equipo en una lista de cabeceras que describa la concatenación de elementos de datos en el certificado.

   A continuación se muestra la lista de cabeceras asociada al contenido de este certificado:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Etiqueta de lista de cabeceras ampliada	Longitud de la lista de cabeceras	Etiqueta CPI	Longitud CPI	Etiqueta CAR	Longitud CAR	Etiqueta CHA	Longitud CHA	Etiqueta EOV	Longitud EOV	Etiqueta CHR	Longitud CHR	Etiqueta de clave pública (construida)	Longitud de los DO subsiguientes	Etiqueta del módulo	Longitud del módulo	Etiqueta del exponente público	Longitud del exponente público

2. La «referencia a la autoridad de certificación» (CAR) sirve para identificar a la CA que expide el certificado, de manera que el elemento de datos se puede utilizar simultáneamente como un identificador de la clave de la autoridad, para señalar la clave pública de la autoridad de certificación (la codificación se explica más adelante, cuando se habla del identificador de clave).

3. La «autorización del titular del certificado» (CHA) sirve para identificar los derechos que posee el titular del certificado. Consta del identificador de la aplicación de tacógrafo y del tipo de equipo a que se refiere el certificado (con arreglo al elemento de datos `EquipmentType`, «00» para un Estado miembro).

4. La «referencia al titular del certificado» (CHR) sirve para identificar de forma inequívoca al titular del certificado, de manera que el elemento de datos se puede utilizar simultáneamente como un identificador de clave de sujeto para señalar la clave pública del titular del certificado.

5. Los identificadores de clave permiten identificar de forma inequívoca al titular del certificado y a las autoridades de certificación. Los identificadores de clave se codifican de la manera siguiente:

5.1. Equipo (VU o tarjeta):

Dato	Nº de serie del equipo	Fecha	Tipo	Fabricante
Longitud	4 bytes	2 bytes	1 byte	1 byte
Valor	Número entero	Codificación BCD mm aa	Específico del fabricante	Código del fabricante

En el caso de una VU, el fabricante, cuando solicita un certificado, puede o no conocer la identificación del equipo en el que se introducirán las claves.

En el primer caso, el fabricante enviará la identificación del equipo, junto con la clave pública, a la autoridad de certificación de su Estado miembro. El certificado que ésta expida contendrá la identificación del equipo. El fabricante debe cerciorarse de que las claves y el certificado se introducen en el equipo que corresponde. El identificador de clave tiene la forma arriba descrita.

En caso contrario, el fabricante debe identificar de forma inequívoca cada solicitud de certificado y enviar dicha identificación, junto con la clave pública, a la autoridad de certificación de su Estado miembro. El certificado que ésta expida contendrá la identificación de la solicitud. Una vez se haya instalado la clave en el equipo, el fabricante, por su parte, debe comunicar a la autoridad de su Estado miembro la asignación de la clave al equipo (es decir, la identificación de la solicitud del certificado, la identificación del equipo). El identificador de clave posee la forma siguiente:

Dato	Nº de serie de solicitud de certificado	Fecha	Tipo	Fabricante
Longitud	4 bytes	2 bytes	1 byte	1 byte
Valor	Número entero	Codificación BCD mm aa	'FF'	Código del fabricante

5.2. Autoridad de certificación:

Dato	Identificación de la autoridad	Nº de serie de la clave	Información adicional	Identificador
Longitud	4 bytes	1 byte	2 bytes	1 byte

Valor	1 byte código numérico del país 3 bytes código alfanumérico del país	Número entero	Codificación adicional (específica de la CA) 'FF FF' si no se utiliza	'01'

El número de serie de la clave sirve para distinguir las diferentes claves de un Estado miembro en caso de que se cambie la clave.

6. Los responsables de verificar los certificados deberán saber de forma implícita que la clave pública certificada es una clave RSA relevante para los servicios de autenticación, verificación de la firma digital y cifrado para confidencialidad (el certificado no contiene ningún Identificador de Objeto que lo especifique).

3.3.2 *Certificados expedidos*

CSM_018 El certificado expedido es una firma digital con recuperación parcial del contenido del certificado, según la norma ISO/IEC 9796-2 (excepto su anexo A4), y se le añade una «referencia a la autoridad de certificación».

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Con el contenido del certificado = Cc = C_r || C_n

106 bytes 58 bytes

Notas:

1. Este certificado tiene una longitud de 194 bytes.

2. La referencia CAR, oculta por la firma, también se añade, de manera que es posible seleccionar la clave pública de la autoridad de certificación para verificar el certificado.

3. El responsable de verificar el certificado deberá conocer de forma implícita el algoritmo empleado por la autoridad de certificación para firmar el certificado.

4. A continuación se muestra la lista de cabeceras asociada a este certificado expedido:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Etiqueta del certificado CV (Construida)	Longitud de los DO subsiguientes	Etiqueta de firma	Longitud de la firma	Etiqueta de resto	Longitud de resto	Etiqueta CAR	Longitud CAR

3.3.3 *Verificación y apertura del certificado*

La verificación y apertura del certificado consiste en verificar la firma con arreglo a la norma ISO/IEC 9796-2, recuperar el contenido del certificado y la clave pública: X.PK = X.CA.PK $_{o}$ X.C, y verificar la validez del certificado.

CSM_019 Este proceso consta de las siguientes etapas:

Verificación de la firma y recuperación del contenido:

— conocido el X.C, recuperar la firma, X.C = Firma || C_n' || CAR' C_n' y CAR':

	128 bytes	58 bytes	8 bytes

— conocida la referencia CAR', seleccionar la clave pública de la autoridad de certificación (si no se ha hecho antes por otros medios),

— abrir la firma con la clave pública de la CA: Sr'= X.CA.PK [Firma],

— comprobar que Sr' comienza con '6A' y termina con 'BC'

— calcular Cr' y H' a partir de: Sr' = '6 A' || C_r' || H' || 'BC'

		106 bytes		20 bytes	

— Recuperar el contenido C' del certificado = C_r' || C_n',

— comprobar que *Hash*(C') = H'

Si estas comprobaciones arrojan un resultado positivo, el certificado es genuino y su contenido es C'.

Una vez conocido el contenido C', verificación de la validez:

— si procede, comprobar el final de la fecha de validez,

Una vez conocido el contenido C', recuperación y almacenamiento de la clave pública, el identificador de clave, la autorización del titular del certificado y el fin de la validez del certificado:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECANISMO DE AUTENTICACIÓN MUTUA

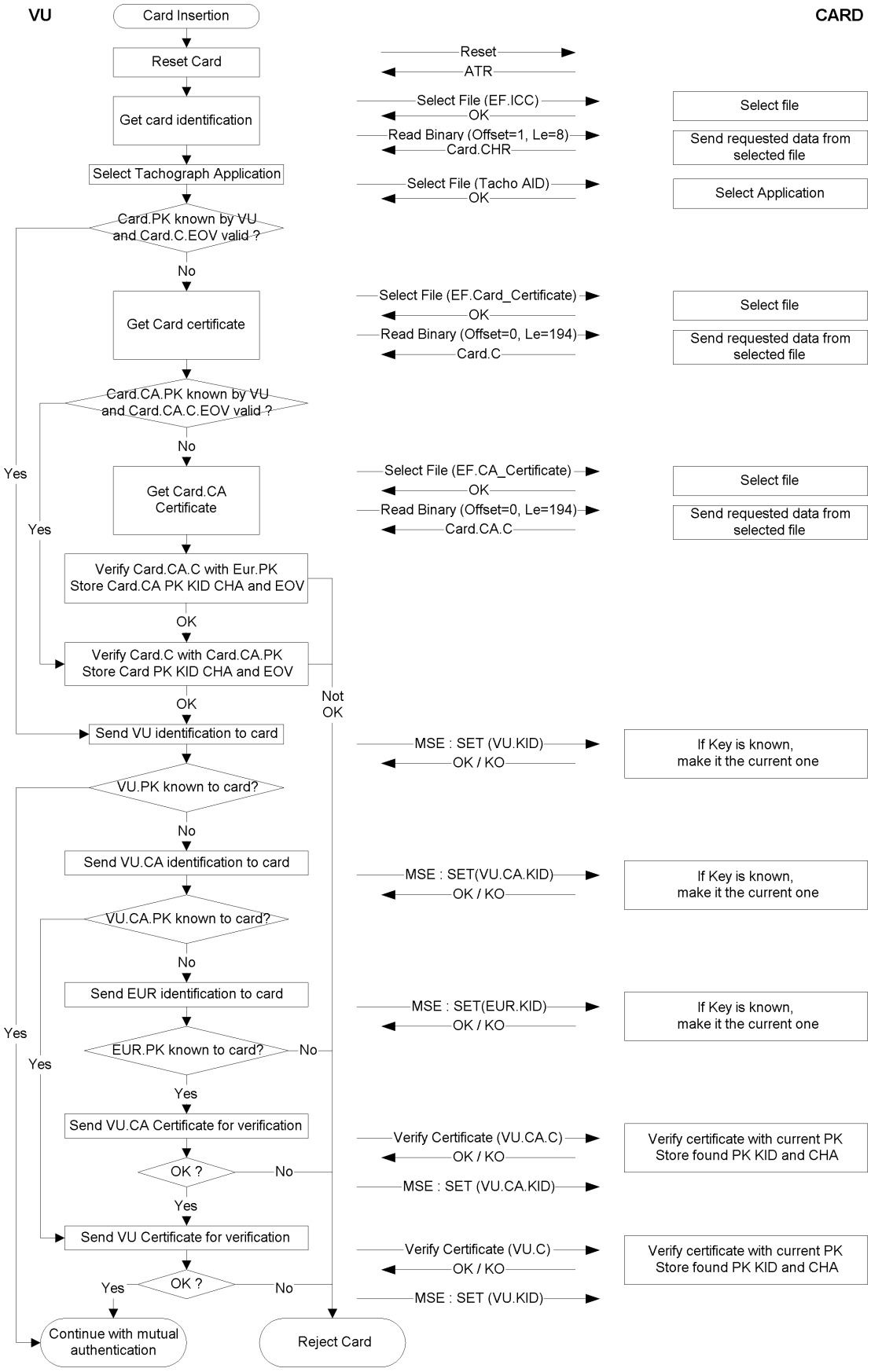
La autenticación mutua entre tarjetas y VU se basa en el siguiente principio:

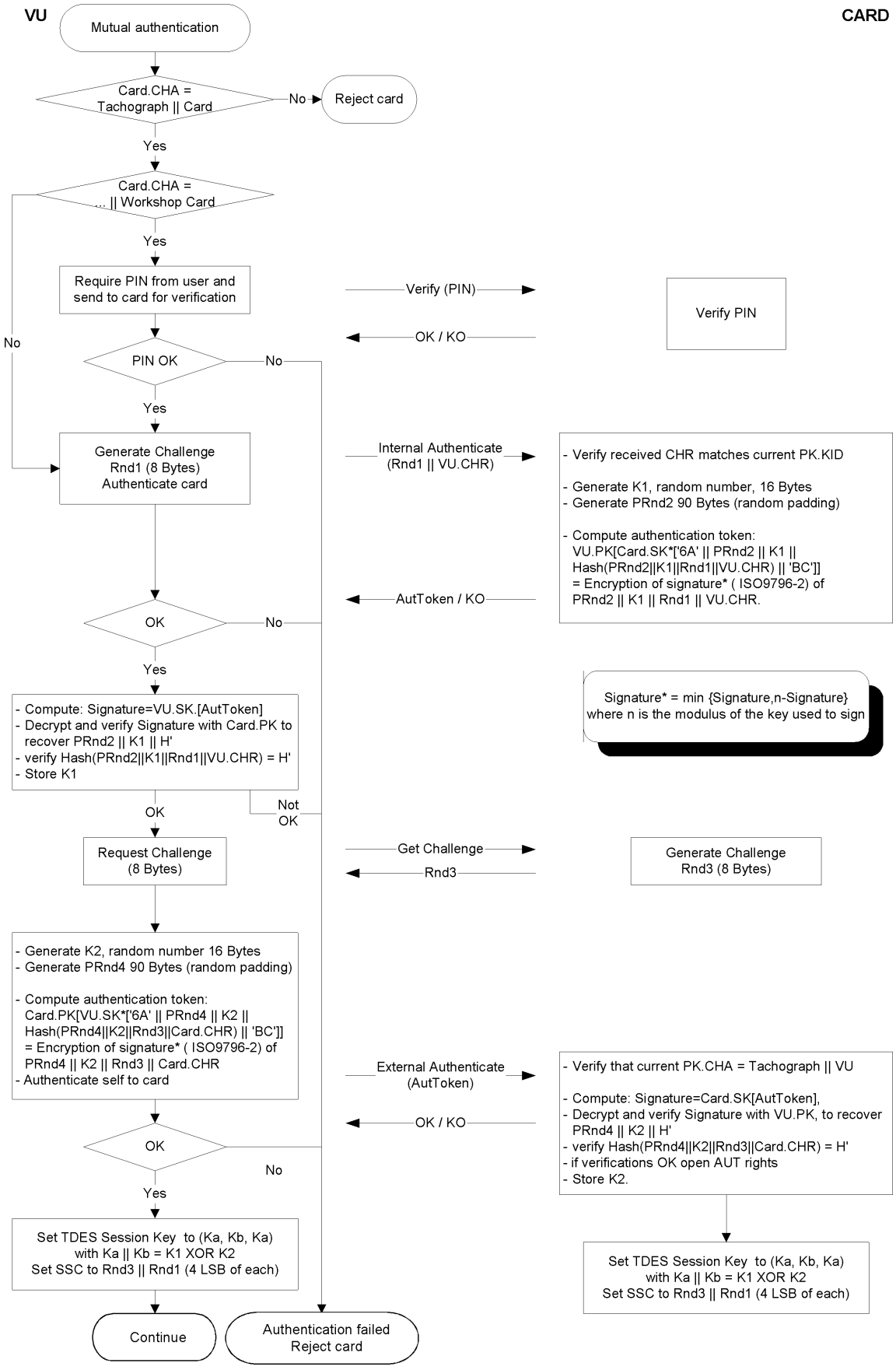
Cada parte deberá demostrar a la otra que está en posesión de un par de claves válido cuya clave pública ha sido certificada por la autoridad de certificación de un Estado miembro, y que dicha autoridad ha sido certificada por la autoridad de certificación europea.

La demostración se lleva a cabo firmando con la clave privada un número aleatorio enviado por la otra parte, quien debe recuperar dicho número cuando verifique esta firma.

El mecanismo lo activa la VU al insertar la tarjeta. Comienza con el intercambio de certificados y la apertura de claves públicas, y termina con la creación de una clave de sesión.

CSM_020 Deberá utilizarse el protocolo siguiente (las flechas indican los comandos y datos que se intercambian [véase el apéndice 2)]:




VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. MECANISMOS DE CONFIDENCIALIDAD, INTEGRIDAD Y AUTENTICACIÓN EN LAS TRANSFERENCIAS DE DATOS ENTRE LA VU Y LAS TARJETAS

5.1. **Mensajería segura**

CSM_021 La integridad de las transferencias de datos entre la VU y las tarjetas estará protegida por un sistema de mensajería segura, de conformidad con los documentos de referencia [ISO/IEC 7816-4] e [ISO/IEC 7816-8].

CSM_022 Cuando haya que proteger los datos durante la transferencia, se añadirá un objeto de datos consistente en una suma de control criptográfica a los objetos de datos que se envíen en el comando o la respuesta. El receptor deberá verificar dicha suma de control criptográfica.

CSM_023 La suma de control criptográfica de los datos enviados en un comando deberá integrar la cabecera del comando y todos los objetos de datos que se envíen ((=>CLA = '0C', y todos los objetos de datos deberán estar englobados en etiquetas donde b1 = 1).

CSM_024 Los bytes correspondientes a la información de estado en la respuesta deberán estar protegidos por una suma de control criptográfica cuando dicha respuesta no contenga un campo de datos.

CSM_025 Las sumas de control criptográficas deberán tener una longitud de 4 bytes.

Así pues, la estructura de comandos y respuestas cuando se utiliza un sistema de mensajería segura es así:

Los DO empleados son un conjunto parcial de los DO de mensajería segura que se describen en la norma ISO/IEC 7816-4:

Etiqueta	Mnemónico	Significado
'81'	T_{PV}	Dato de valor plano no codificado en BER-TLV (con la protección de la suma CC)
'97'	$\mathbf{T_{LE}}$	Valor de Le en el comando no seguro (con la protección de la suma CC)
'99'	T_{SW}	Información de estado (con la protección de la suma CC)
'8E'	T_{CC}	Suma de control criptográfica
'87'	$T_{PI\ CG}$	Byte indicador de relleno || Criptograma (Valor plano no codificado en BER-TLV)

Dado un par de respuestas para un comando no seguro:

Cabecera de comando				Cuerpo del comando		
CLA	INS	P1	P2	[campo L_c]	[campo de datos]	[campo L_e]
cuatro bytes				L bytes, denotados por B_1 a B_L		

Cuerpo de la respuesta	Cola de la respuesta	
[campo de datos]	SW1	SW2
L_r bytes de datos	dos bytes	

El correspondiente par de respuestas para el comando seguro es:

Comando seguro:

Cabecera del comando (CH)				Cuerpo del comando										
CLA	INS	P1	P2	[Nuevo campo L_c]	[Nuevo campo de datos]									[Nuevo campo L_e]
'OC'				Longitud del nuevo campo de datos	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	Campo de datos	'97'	'01'	L_e	'8E'	'04'	CC	

Datos que habrá que integrar en la suma de control = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Bytes de relleno (80.. 00) con arreglo a las normas ISO-IEC 7816-4 e ISO 9797, método 2.

Los DO PV y LE sólo están presentes cuando existen datos correspondientes en el comando no seguro.

Respuesta segura:

1. Caso en que el campo de datos de la respuesta no está vacío y no es necesario protegerlo para garantizar la confidencialidad:

Cuerpo de la respuesta						Cola de la respuesta
[Nuevo campo de datos]						nuevo SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Campo de datos	'8E'	'04'	CC	

Datos que habrá que integrar en la suma de control = T_{PV} || L_{PV} || PV || PB

2. Caso en que el campo de datos de la respuesta no está vacío y debe ser protegido para garantizar la confidencialidad:

Cuerpo de la respuesta						Cola de la respuesta
[Nuevo campo de datos]						nuevo SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Datos que deberá llevar el CG: datos no codificados en BER-TLV y bytes de relleno.

Datos que habrá que integrar en la suma de control = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Caso en que el campo de datos de la respuesta está vacío:

Cuerpo de la respuesta						Cola de la respuesta
[Nuevo campo de datos]						nuevo SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nuevo SW1 SW2	'8E'	'04'	CC	

Datos que habrá que integrar en la suma de control = T_{SW} || L_{SW} || SW || PB

5.2. Tratamiento de los errores de mensajería segura

CSM_026 Si la tarjeta de tacógrafo detecta un error SM mientras está interpretando un comando, los bytes de estado tendrán que ser devueltos sin SM. De acuerdo con la norma ISO/IEC 7816-4, se definen los siguientes bytes de estado para indicar errores SM:

'66 88': Ha fallado la verificación de la suma de control criptográfica,

'69 87': Faltan los objetos de datos SM que se esperaban,

'69 88': Objetos de datos SM incorrectos.

CSM_027 Si la tarjeta de tacógrafo devuelve bytes de estado sin DO SM o con un DO SM erróneo, la VU tendrá que interrumpir la sesión.

5.3. Algoritmo para calcular sumas de control criptográficas

CSM_028 Las sumas de control criptográficas se construyen utilizando MAC según ANSI X9.19, con DES:

— etapa inicial: el bloque de control inicial y0 es E(Ka, SSC);

— etapa secuencial: los bloques de control y1,.., yn se calculan utilizando Ka;

— etapa final: la suma de control criptográfica se calcula a partir del último bloque de control yn de la manera siguiente: E(Ka, D(Kb, yn)).

donde E() significa cifrado con DES, y D() significa descifrado con DES.

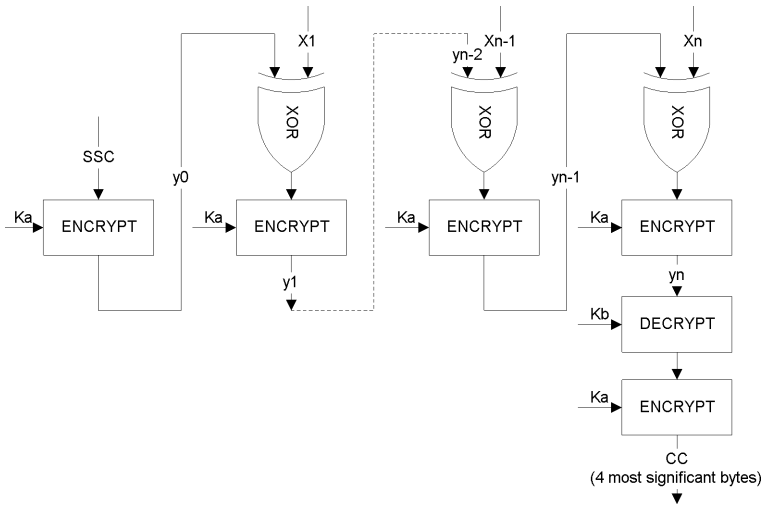
Se transfieren los cuatro bytes más significativos de la suma de control criptográfica.

CSM_029 El contador de la secuencia de envío (SSC) deberá iniciarse durante el procedimiento de acuerdo de la clave:

SSC inicial: Rnd3 (los 4 bytes menos significativos) || Rnd1 (los 4 bytes menos significativos).

CSM_030 El contador de la secuencia de envío deberá incrementarse en una unidad cada vez antes de que se calcule el MAC (es decir, el SSC para el primer comando es el SSC inicial + 1, el SSC para la primera respuesta es el SSC inicial — 2).

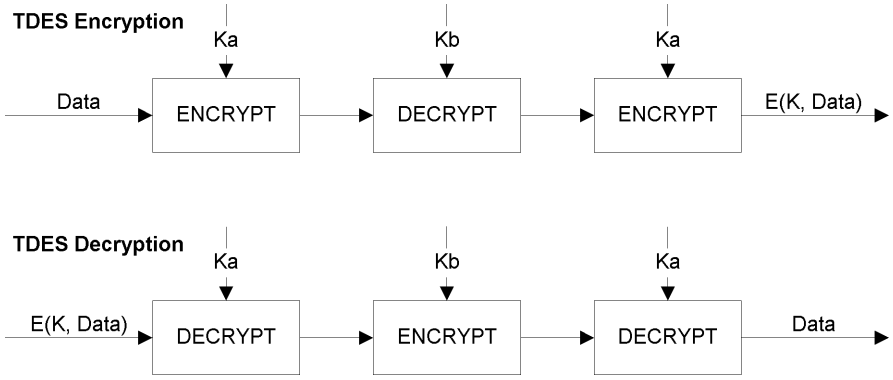
El gráfico siguiente muestra el método de cálculo del MAC:



5.4. Algoritmo para calcular criptogramas con los que mantener la confidencialidad de los DO

CSM_031 Los criptogramas se calculan utilizando el algoritmo TDEA en el modo de funcionamiento TCBC, de acuerdo con los documentos de referencia TDES y TDES-OP y con el vector nulo como bloque de valor inicial.

El gráfico siguiente muestra la aplicación de claves en TDES:



6. MECANISMOS DE FIRMA DIGITAL PARA LA TRANSFERENCIA DE DATOS

CSM_032 El equipo dedicado inteligente (IDE) almacena en un archivo físico los datos recibidos de un equipo (VU o tarjeta) durante una sesión de descarga. Dicho archivo debe contener los certificados MSi.C y EQT.C. El archivo contiene además firmas digitales de bloques de datos, tal y como se especifica en el apéndice 7, apartado Protocolos de transferencia de datos.

CSM_033 Las firmas digitales de los datos transferidos deberán utilizar un esquema de firma digital con apéndice, de manera que los datos transferidos puedan leerse sin necesidad de descifrarlos, si se desea.

6.1. Generación de firmas

CSM_034 La generación de firmas de datos por parte del equipo deberá seguir el esquema de firma con apéndice que se define en el documento de referencia [PKCS1] con la función de comprobación aleatoria SHA-1:

Firma = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(datos))]

PS = Cadena de octetos de relleno con un valor 'FF' tal que la longitud sea 128.

DER(SHA-1(M)) es la codificación de la identificación del algoritmo para la función de comprobación aleatoria y el valor de comprobación aleatoria, con el fin de obtener un valor ASN.1 del tipo DigestInfo (reglas de codificación distinguidas):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Valor de comprobación aleatoria.

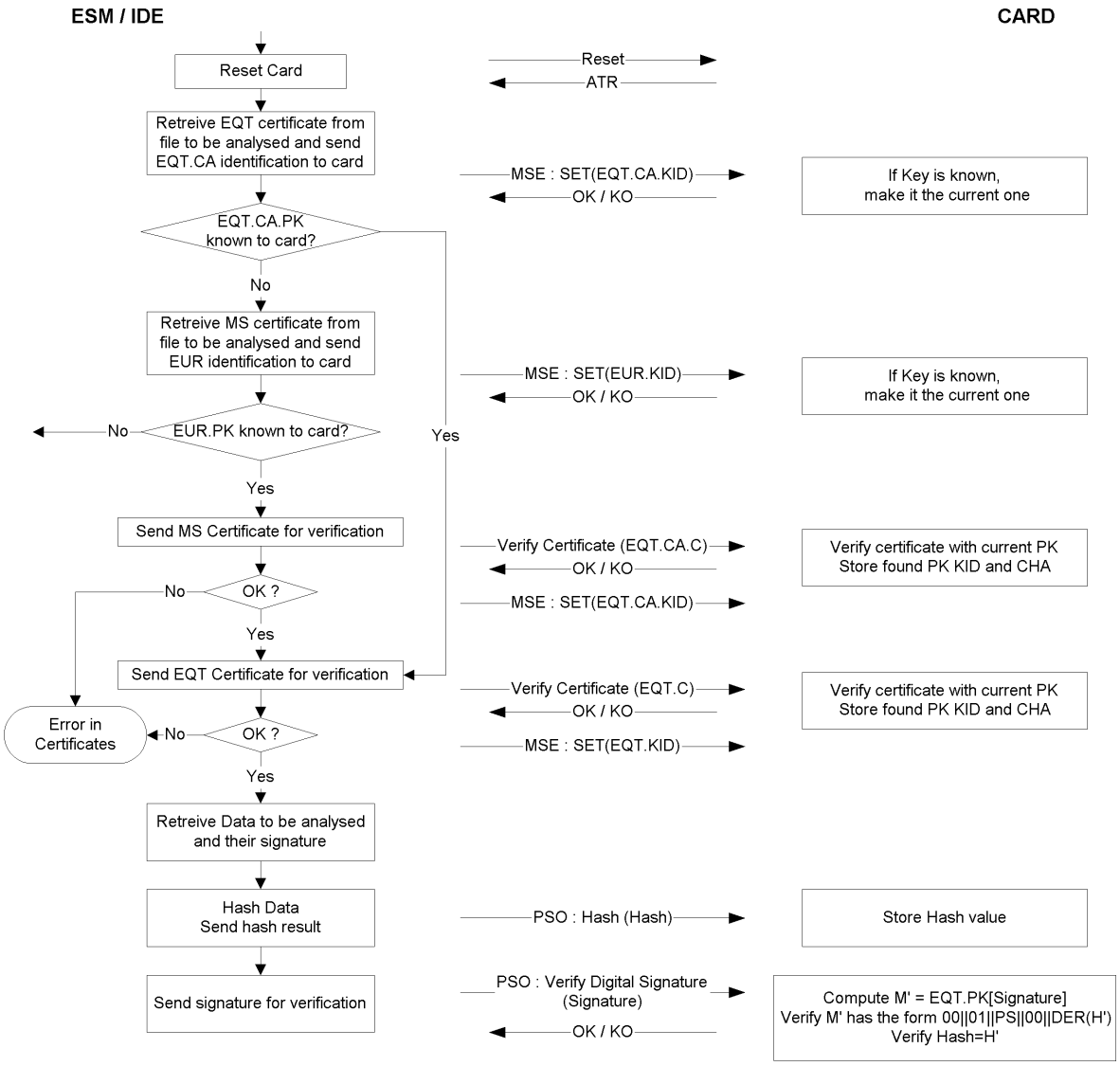
6.2. Verificación de firmas

CSM_035 La verificación de la firma en los datos transferidos deberá seguir el esquema de firma con apéndice que se define en el documento de referencia [PKCS1] con la función de comprobación aleatoria SHA-1:

El responsable de verificación debe conocer independientemente (y confiar en) la clave pública europea EUR.PK.

La tabla siguiente muestra el protocolo que una IDE que incorpore una tarjeta de control puede seguir para verificar la integridad de los datos transferidos y almacenados en el ESM (medio de almacenamiento externo). La tarjeta de control sirve para descifrar las firmas digitales. En este caso, puede que esta función no esté implementada en la IDE.

El equipo que ha transferido y firmado los datos que han de analizarse se denota por EQT.



PARTE B

SISTEMA DE TACÓGRAFO DE SEGUNDA GENERACIÓN

7. INTRODUCCIÓN

7.1. **Referencias**

En esta parte del presente apéndice aparecen las siguientes referencias:

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), 26 de noviembre de 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), julio de 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. Tercera edición 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations. Segunda edición 2004-06-01
ISO 8825-1	ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Cuarta edición, 2008-12-15
ISO 9797-1	ISO/IEC 9797-1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher. Segunda edición, 2011-03-01
ISO 10116	ISO/IEC 10116, Information technology — Security techniques — Modes of operation of an *n*-bit block cipher. Tercera edición, 2006-02-01
ISO 16844-3	ISO/IEC 16844-3, Road vehicles — Tachograph systems — Part 3: Interfaz del sensor de movimiento. Primera edición de 2004, incluida la correción técnica de errores 1 2006
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, marzo de 2009
RFC 5639	Elliptic Curve Cryptography (ECC) — Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), mayo de 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, marzo de 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, versión 2.00, 2012-06-28

7.2. **Notaciones y abreviaturas**

En el presente apéndice se emplean las siguientes notaciones y términos abreviados:

AES	Advanced Encryption Standard (/norma de cifrado avanzado)
CA	Certification authority (/autoridad de certificación),
CAR	Certificate Authority Reference (/referencia a la autoridad de certificación)
CBC	Cipher Block Chaining (mode of operation) [/cifrado progresivo (modo de funcionamiento)]

CH	Command Header (/cabecera de comando),
CHA	Certificate Holder Authorisation (/autorización del titular del certificado)
CHR	Certificate Holder Reference (/referencia al titular del certificado)
CV	Constant Vector (/vector constante)
DER	Distinguished Encoding Rules (/reglas de codificación distinguidas)
DO	Data object (/objeto de datos)
DSRC	Dedicated Short Range Communication (/comunicaciones especializadas de corto alcance)
ECC	Elliptic Curve Cryptography (/criptografía de curva elíptica)
ECDSA	Elliptic Curve Digital Signature Algorithm (/algoritmo de firma digital de curva elíptica)
ECDH	Elliptic Curve Diffie-Hellman (key agreement algorithm) [/curva elíptica Diffie-Hellman (algoritmo de acuerdo de la clave)
EGF	External GNSS Facility (/dispositivo GNSS externo)
EQT	Equipment (/equipo)
IDE	Intelligent Dedicated Equipment (/equipo especializado inteligente)
K_M	Clave maestra del sensor de movimiento que permite aparear una unidad instalada en el vehículo con un sensor de movimiento
K_{M-VU}	Clave introducida en unidades de vehículo que permite a una VU derivar la clave maestra del sensor de movimiento si se introduce una tarjeta de taller en la VU
K_{M-WC}	Clave introducida en tarjetas de centro de ensayo que permite a una VU derivar la clave maestra del sensor de movimiento si se introduce una tarjeta de taller en la VU
MAC	Message Authentication Code (/código de autenticación de mensajes)
MoS	Motion Sensor (/sensor de movimiento)
MSB	Most Significant Bit (/bit más significativo)
PKI	Public Key Infrastructure (/infraestructura de clave pública)
RCF	Remote Communication Facility (/instalación de comunicación remota)
SSC	Send sequence counter (/contador de la secuencia de envío)
SM	Secure Messaging (/mensajeria segura)
TDES	Triple Data Encryption Standard (/norma de cifrado triple de datos)
TLV	Tag Length Value (/valor de longitud de la etiqueta)
VU	Vehicle Unit (/unidad instalada en el vehículo),
X.C	El certificado de clave pública de un usuario X
X.CA	La autoridad de certificación que haya expedido el certificado del usuario X
X.CAR	La referencia de la autoridad de certificación mencionada en el certificado del usuario X
X.CHR	La referencia al titular del certificado mencionada en el certificado del usuario X
X.PK	Clave pública de un usuario X
X.SK	Clave privada de un usuario X
$X.PK_{eph}$	Clave pública efímera de un usuario X
$X.SK_{eph}$	Clave privada efímera de un usuario X
'xx'	Un valor hexadecimal
||	Operador de concatenación.

7.3. **Definiciones**

Las definiciones de los términos utilizados en el presente apéndice figuran en la sección I del anexo 1C.

8. SISTEMAS Y ALGORITMOS CRIPTOGRÁFICOS

8.1. **Sistemas criptográficos**

CSM_38 Las unidades instaladas en los vehículos y las tarjetas de tacógrafo deberán emplear un sistema criptográfico de curva elíptica de clave pública para ofrecer los siguientes servicios de seguridad:

— autenticación mutua entre una unidad instalada en el vehículo y una tarjeta;

— acuerdo de claves de sesión AES entre una unidad instalada en el vehículo y una tarjeta;

— garantía de la autenticidad, integridad y no rechazo de los datos descargados desde unidades instaladas en los vehículos o tarjetas de tacógrafo a medios externos.

CSM_39 Las unidades instaladas en los vehículos y los dispositivos GNSS externos deberán emplear un sistema criptográfico de curva elíptica de clave pública para ofrecer los siguientes servicios de seguridad:

— acoplamiento de una unidad instalada en el vehículo y un dispositivo GNSS externo;

— autenticación mutua entre una unidad instalada en el vehículo y un dispositivo GNSS externo;

— acuerdo de una clave de sesión AES entre una unidad instalada en el vehículo y un dispositivo GNSS externo.

CSM_40 Las unidades instaladas en los vehículos y las tarjetas de tacógrafo deberán emplear un sistema criptográfico AES para ofrecer los siguientes servicios de seguridad:

— garantía de la autenticidad e integridad de los datos intercambiados entre una unidad instalada en el vehículo y una tarjeta de tacógrafo;

— cuando corresponda, garantía de la confidencialidad de los datos intercambiados entre una unidad instalada en el vehículo y una tarjeta de tacógrafo.

CSM_41 Las unidades instaladas en los vehículos y los dispositivos GNSS externos deberán emplear un sistema criptográfico AES para ofrecer los siguientes servicios de seguridad:

— garantía de la autenticidad e integridad de los datos intercambiados entre una unidad instalada en el vehículo y un dispositivo GNSS externo.

CSM_42 Las unidades instaladas en los vehículos y los sensores de movimiento deberán emplear un sistema criptográfico AES para ofrecer los siguientes servicios de seguridad:

— emparejamiento de una unidad instalada en el vehículo y un sensor de movimiento;

— autenticación mutua entre una unidad instalada en el vehículo y un sensor de movimiento;

— garantía de la confidencialidad de los datos intercambiados entre una unidad instalada en el vehículo y un sensor de movimiento.

CSM_43 Las unidades instaladas en los vehículos y las tarjetas de control deberán emplear un sistema criptográfico AES para ofrecer los siguientes servicios de seguridad en la interfaz de comunicación remota.

— garantía de la autenticidad e integridad de los datos transmitidos desde una unidad instalada en el vehículo a una tarjeta de control.

Notas:

— Hablando con propiedad, los datos se transmiten desde una unidad instalada en el vehículo a un interrogador remoto bajo el control de un controlador a través de una instalación de comunicación remota que puede ser interna o externa a la VU, véase el apéndice 14. No obstante, el interrogador remoto envía los datos recibidos a una tarjeta de control para descifrado y validación de autenticidad. Desde el punto de vista de la seguridad, la instalación de comunicación remota y el interrogador remoto son plenamente transparentes.

— Una tarjeta de taller ofrece los mismos servicios de seguridad para la interfaz DSRC que una tarjeta de control. Esto permite a un taller validar el funcionamiento correcto de la interfaz de comunicación remota de una VU, incluida la seguridad. Remítase a la sección para 9.2.2 mayor información.

8.2. **Algoritmos criptográficos**

8.2.1 *Algoritmos simétricos*

CSM_44 Las unidades instaladas en los vehículos, las tarjetas de tacógrafo, los sensores de movimiento y los dispositivos GNSS externos admitirán el algoritmo AES según se define en [AES], con longitudes de clave de 128, 192 y 256 bits.

8.2.2 *Algoritmos asimétricos y parámetros de dominio normalizados*

CSM_45 Las unidades instaladas en los vehículos, las tarjetas de tacógrafo y los dispositivos GNSS externos admitirán criptografía de curva elíptica con un tamaño de clave de 256, 384 y 512/521 bits.

CSM_46 Las unidades instaladas en los vehículos, las tarjetas de tacógrafo y los dispositivos GNSS externos admitirán el algoritmo de firma ECDSA, según se especifica en [DSS].

CSM_47 Las unidades instaladas en los vehículos, las tarjetas de tacógrafo y los dispositivos GNSS externos admitirán el algoritmo de acuerdo de la clave ECKA-EG, según se especifica en la directriz técnica [TR 03111].

CSM_48 Las unidades instaladas en los vehículos, las tarjetas de tacógrafo y los dispositivos GNSS externos admitirán todos los parámetros de dominio normalizados especificados en la Table 1 siguiente para criptografía de curva elíptica.

Tabla 1

Parámetros de dominio normalizados

Nombre	Tamaño (bits)	Referencia	Identificador de objeto
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Nota: los identificadores de objeto mencionados en la última columna de la Table 1 vienen especificados en [RFC 5639] para las curvas Brainpool y en [RFC 5480] para las curvas NIST.

Ejemplo 1: el identificador de objeto de la curva BrainpoolP256r1 es `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

O en notación de puntos: `1.3.36.3.3.2.8.1.1.7`.

Ejemplo 2: el identificador de objeto de la curva NIST P-384 es

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

O en notación de puntos: `1.3.132.0.34`.

8.2.3 *Algoritmos de comprobación aleatoria*

CSM_49 Las unidades instaladas en los vehículos y las tarjetas de tacógrafo admitirán los algoritmos HA-256, SHA-384 y SHA-512 especificados en [SHS].

8.2.4 *Conjuntos de cifrado*

CSM_50 Si se utilizan simultáneamente un algoritmo simétrico, un algoritmo asimétrico y/o un algoritmo de comprobación aleatoria para formar un protocolo de seguridad, sus longitudes de clave y tamaños de algoritmo de autenticación respectivos serán de fortaleza aproximadamente equivalente. La Table 2 indica los descriptores permitidos:

Tabla 2

Conjuntos de cifrado permitidos

Id del conjunto de cifrado	Tamaño de clave ECC (bits)	Longitud de clave AES (bits)	Algoritmo de comprobación aleatoria	Longitud de MAC (bytes)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Nota: Los tamaños de clave ECC de 512 bits y 521 bits se consideran de fortaleza equivalente a todos los efectos en el presente apéndice.

9. CLAVES Y CERTIFICADOS

9.1. **Pares asimétricos de claves y certificados de clave pública**

9.1.1 *Generalidades*

Nota: las claves descritas en esta sección se utilizan para la autenticación mutua y la mensajería segura entre unidades instaladas en los vehículos y tarjetas de tacógrafo, así como entre unidades instaladas en los vehículos y dispositivos GNSS externos. Estos procesos se describen en detalle en los capítulos 10 y 11 de este apéndice.

CSM_51 En el sistema europeo de tacógrafo inteligente, los pares de claves ECC y los certificados correspondientes se generarán y gestionarán mediante tres niveles jerárquicos funcionales:

— Nivel europeo

— Nivel de Estado miembro

— Nivel de equipo.

CSM_52 En la totalidad del sistema de Tacógrafo Inteligente Europeo, las claves públicas y privadas y los certificados se generarán, gestionarán y comunicarán mediante métodos normalizados y seguros.

9.1.2 *Nivel europeo*

CSM_53 En el nivel europeo deberá generarse un único par de claves ECC designado EUR compuesto de una clave privada (EUR:SK) y de una clave pública (EUR.PK). Este par de claves formará el par de claves raíz de la totalidad del Tacógrafo Inteligente Europeo PKI. Esta tarea será gestionada por la Autoridad del Certificado Raíz Europeo (ERCA), bajo la autoridad y responsabilidad de la Comisión Europea.

CSM_54 La ERCA utilizará la clave privada europea para firmar un certificado raíz (autofirmado) de la clave pública europea y comunicará este certificado raíz europeo a todos los Estados miembros.

CSM_55 La ERCA utilizará la clave privada europea para firmar los certificados de las claves públicas de los Estados miembros a solicitud de estos. La ERCA llevará un registro de todos los certificados de clave pública de los Estados miembros que haya firmado.

CSM_56 Como se indica en la Figure 1 de la sección 9.1.7, la ERCA generará un nuevo par de claves raíz europeo cada 17 años. Siempre que la ERCA genera un nuevo par de claves raíz europeo, creará un nuevo certificado raíz autofirmado para la nueva clave pública europea. El período de validez de un certificado raíz europeo será de 34 años y 3 meses.

Nota: La introducción de un nuevo par de claves raíz implica asimismo que la ERCA genere una nueva clave maestra del sensor de movimiento y una nueva clave maestra DSRC, véanse las secciones 9.2.1.2 y 9.2.2.2.

CSM_57 Antes de generar un nuevo par de claves raíz europeo, la ERCA efectuará un análisis de la fortaleza criptográfica necesaria para el nuevo par de claves, habida cuenta de la necesidad de garantizar su seguridad durante los 34 años siguientes. En caso necesario, la ERCA cambiará a un conjunto de cifrado más fuerte que el actual, tal como se especifica en CSM_50.

CSM_58 Siempre que genere un nuevo par de claves raíz europeo, la ERCA creará un certificado de enlace para la nueva clave pública europea y la firmará con la clave privada europea anterior. El período de validez del certificado de enlace será de 17 años. Lo anterior se indica asimismo en la Figure 1 de la sección 9.1.7.

Nota: Dado que un certificado de enlace contiene la clave pública de la generación ERCA X y está firmado con la clave privada de la generación ERCA X-1, el certificado de enlace ofrece a los equipos de la generación X-1 un método de confianza en los equipos de la generación X.

CSM_59 La ERCA no utilizará la clave privada de un par de claves raíz para ningún fin a partir del momento en que adquiera validez un nuevo certificado raíz de clave.

CSM_60 La ERCA dispondrá en cualquier momento de las siguientes claves criptográficas y certificados:

— El par de claves EUR actual y el certificado correspondiente.

— Todos los certificados EUR anteriores que deberán utilizarse para la verificación de certificados MSCA que son todavía válidos.

— Los certificados de enlace para todas las generaciones de certificados EUR excepto el primero.

9.1.3 *Nivel del Estado miembro*

CSM_61 Al nivel del Estado miembro, todos los Estados miembros a los que se solicite la firma de certificados de tarjeta de tacógrafo generarán uno o varios pares de claves ECC únicos designados MSCA_Card. Todos los Estados miembros a los que se solicite la firma de certificados para unidades instaladas en los vehículos o dispositivos GNSS externos generarán uno o varios pares de claves ECC únicos designados MSCA_VU-EGF.

CSM_62 La tarea de generar pares de claves del Estado miembro será gestionada por una Autoridad de Certificación del Estado miembro (MSCA). Siempre que una MSCA genere un par de claves de un Estado miembro, enviará la clave pública a la ERCA a fin de obtener un certificado correspondiente del Estado miembro firmado por la ERCA.

CSM_63 Una MSCA seleccionará la fortaleza de un par de claves de un Estado miembro igual a la fortaleza del par de claves raíz europeo utilizado para firmar el certificado correspondiente del Estado miembro.

CSM_64 Un par de claves MSCA_VU-EGF, si está presente, estará compuesto por la clave privada MSCA_VU-EGF.SK y la clave pública MSCA_VU-EGF.PK. Una MSCA utilizará la clave privada MSCA_VU-EGF.SK exclusivamente para firmar los certificados de clave pública de las unidades instaladas en los vehículos y los dispositivos GNSS externos.

CSM_65 Un par de claves MSCA_Card estará compuesto por la clave privada MSCA_Card.SK y la clave pública MSCA_Card.PK. Una MSCA utilizará la clave privada MSCA_Card.SK exclusivamente para firmar los certificados de clave pública y las tarjetas de tacógrafo.

CSM_66 Una MSCA llevará un registro de todos los certificados VU, los certificados de dispositivo GNSS externo y los certificados de tarjeta firmados, junto con la identificación del equipo al que esté destinado cada certificado.

CSM_67 El período de validez de un certificado MSCA_VU-EGF será de 17 años y 3 meses. El período de validez de un certificado MSCA_Card será de 7 años y 1 mes.

CSM_68 Tal como muestra la Figure 1 de la sección 9.1.7, la clave privada de un par de claves MSCA_VU-EGF y la clave privada de un par de claves MSCA_Card tendrán un período de uso de la clave de dos años.

CSM_69 Una MSCA no utilizará la clave privada de un par de claves MSCA_VU-EGF para ningún fin a partir del momento en que su período de uso haya finalizado. Una MSCA tampoco utilizará la clave privada de un par de claves MSCA_Card para ningún fin a partir del momento en que su período de uso haya finalizado.

CSM_70 Una MSCA dispondrá en cualquier momento de las siguientes claves criptográficas y certificados:

— El par de claves MSCA_Card actual y el certificado correspondiente.

— Todos los certificados MSCA_Card anteriores que deberán utilizarse para la verificación de los certificados de tarjetas de tacógrafo que son todavía válidos.

— El certificado EUR actual necesario para la verificación del certificado MSCA actual.

— Todos los certificados EUR anteriores necesarios para la verificación de certificados MSCA que son todavía válidos.

CSM_71 Si se solicita de una MSCA que firme certificados para unidades instaladas en los vehículos o dispositivos GNSS externos, la MSCA dispondrá además de las siguientes claves y certificados:

— El par de claves MSCA_VU-EGF actual y el certificado correspondiente.

— Todas las claves públicas MSCA_VU-EGF anteriores que deberán utilizarse para la verificación de los certificados de VU o de dispositivos GNSS externos que son todavía válidos.

9.1.4 *Nivel de equipo: Unidades instaladas en los vehículos*

CSM_72 Para cada unidad instalada en el vehículo se generarán dos pares de claves ECC únicos, designados VU_MA y VU_Sign. Esta tarea es efectuada por los fabricantes de VU. Siempre que se genere un nuevo par de claves VU, la parte que genere la clave enviará la clave pública a la MSCA del país en el que resida a fin de obtener el certificado VU correspondiente firmado por la MSCA. La clave privada será utilizada solamente por la unidad instalada en el vehículo.

CSM_73 Los certificados VU_MA y VU_Sign de una unidad concreta instalada en el vehículo tendrán la misma fecha de validez.

CSM_74 Un fabricante de VU seleccionará la fortaleza de un par de claves VU igual a la fortaleza del par de claves MSCA utilizado para firmar el certificado correspondiente de la VU.

CSM_75 Una unidad instalada en el vehículo utilizará su par de claves VU_MA, compuesto por la clave privada VU_MA.SK y la clave pública VU_MA.PK, exclusivamente para efectuar la autenticación de la VU en tarjetas de tacógrafo y dispositivos GNSS externos, tal como se especifica en las secciones 10.3 y 11.4 del presente apéndice.

CSM_76 Una unidad instalada en el vehículo deberá poder generar pares de claves ECC efímeros y utilizará un par de claves efímero exclusivamente para establecer la clave de sesión con una tarjeta de tacógrafo o dispositivo GNSS externo, tal como se especifica en las secciones 10.4 y 11.4 del presente apéndice.

CSM_77 Una unidad instalada en el vehículo utilizará la clave privada VU_Sign.SK de su par de claves VU_Sign exclusivamente para firmar archivos de datos descargados, tal como se especifica en el capítulo 14 del presente apéndice. La clave pública VU_Sign.PK correspondiente se utilizará exclusivamente para verificar las firmas creadas por la unidad instalada en el vehículo.

CSM_78 Como se indica en la Figure 1 de la sección 9.1.7, el período de validez de un certificado VU_MA será de 15 años y 3 meses. El período de validez de un certificado VU_Sign también será de 15 años y 3 meses.

Notas:

— El período de validez ampliado de un certificado VU_Sign permite a una unidad instalada en el vehículo crear firmas válidas en datos descargados durante los tres primeros meses posteriores a su caducidad, de conformidad con lo dispuesto en el Reglamento (UE) nº 581/2010.

— El período de validez ampliado de un certificado VU_MA es necesario para permitir la autenticación de la VU con una tarjeta de control o una tarjeta de empresa durante los tres primeros meses posteriores a su caducidad, de tal modo que sea posible efectuar una descarga de datos.

CSM_79 Una unidad instalada en el vehículo no utilizará la clave privada de un par de claves VU para ningún fin una vez caducado el certificado correspondiente.

CSM_80 Los pares de claves VU (excepto los pares de claves efímeros) y los certificados correspondientes de una unidad concreta instalada en el vehículo no se sustituirán ni renovarán en el campo una vez puesta en funcionamiento la unidad instalada en el vehículo.

Notas:

— Los pares de claves efímeros no están incluidos en este requisito, ya que una UV genera un nuevo par de claves efímero cada vez que se efectúa una autenticación del chip y un acuerdo de claves de sesión, véase la sección 10.4. Obsérvese que los pares de claves efímeros carecen de certificados correspondientes.

— Este requisito no prohíbe la posibilidad de sustituir pares de claves VU estáticos durante una renovación o reparación en un entorno seguro controlado por el fabricante de la VU.

CSM_81 Una vez puestas en funcionamiento, las unidades instaladas en los vehículos contendrán las siguientes claves criptográficas y certificados:

— La clave privada VU_MA y el certificado correspondiente.

— La clave privada VU_Sign y el certificado correspondiente.

— El certificado MSCA_VU-EGF que contiene la clave pública MSCA_VU-EGF que deberá utilizarse para la verificación del certificado VU_MA y el certificado VU_Sign.

— El certificado EUR que contiene la clave pública EUR.PK que deberá utilizarse para la verificación del certificado MSCA_VU-EGF.

— El certificado EUR cuyo período de validez es directamente anterior al período de validez del certificado EUR que deberá utilizarse para verificar el certificado MSCA_VU-EGF, si existe.

— El certificado de enlace que asocia estos dos certificados EUR, si existe.

CSM_82 Además de las claves criptográficas y los certificados enumerados en CSM_81, las unidades instaladas en los vehículos deberán contener asimismo las claves y certificados especificados en la parte A del presente apéndice de forma que una unidad instalada en el vehículo pueda interactuar con las tarjetas de tacógrafo de primera generación.

9.1.5 *Nivel de equipo: Tarjetas de tacógrafo*

CSM_83 Para cada tarjeta de tacógrafo se generará un par de claves ECC único, designado Card_MA. Además, para cada tarjeta de conductor y cada tarjeta de taller se generará un segundo par de claves ECC único, designado Card_Sign. Esta tarea puede ser efectuada por los fabricantes de tarjetas o los personalizadores de tarjetas. Siempre que se genere un nuevo par de claves de tarjeta, la parte que genere la clave enviará la clave pública a la MSCA del país en el que resida a fin de obtener el certificado de la tarjeta correspondiente firmado por la MSCA. La clave privada será utilizada solamente por la tarjeta de tacógrafo.

CSM_84 Los certificados Card_MA y Card_Sign de una tarjeta de conductor o de una tarjeta de taller concretas tendrán la misma fecha de validez.

CSM_85 Un fabricante de tarjetas o un personalizador de tarjetas seleccionará la fortaleza de un par de claves de tarjeta igual a la fortaleza del par de claves MSCA utilizado para firmar el certificado correspondiente de la tarjeta.

CSM_86 Una tarjeta de tacógrafo utilizará su par de claves Card_MA, compuesto por la clave privada Card_MA.SK y la clave pública Card_MA.PK, exclusivamente para efectuar la autenticación mutua y establecer la clave de sesión con las unidades instaladas en los vehículos, tal como se especifica en las secciones 10.3 y 10.4 del presente apéndice.

CSM_87 Una tarjeta de conductor o tarjeta de taller utilizará la clave privada Card_Sign.SK de su par de claves Card_Sign exclusivamente para firmar archivos de datos descargados, tal como se especifica en el capítulo 14 del presente apéndice. La clave pública Card_Sign.PK correspondiente se utilizará exclusivamente para verificar las firmas creadas por la tarjeta.

CSM_88 El período de validez de un certificado Card_MA será el siguiente:

— Para las tarjetas de conductor: 5 años

— Para las tarjetas de empresa: 2 años

— Para las tarjetas de control: 2 años

— Para las tarjetas de taller: 1 año

CSM_89 El período de validez de un certificado Card_Sign será el siguiente:

— Para las tarjetas de conductor: 5 años y 1 mes

— Para las tarjetas de taller: 1 año y 1 mes

Nota: El período de validez ampliado de un certificado Card_Sign permite a una tarjeta de conductor crear firmas válidas en datos descargados durante el primer mes posterior a su caducidad. Esto es necesario de conformidad con el Reglamento (UE) nº 581/2010 que exige que sea posible efectuar una descarga de datos de una tarjeta de conductor hasta transcurridos 28 días desde el último registro de datos.

CSM_90 Los pares de claves y los certificados correspondientes de una tarjeta de tacógrafo concreta no se sustituirán ni renovarán una vez expedida la tarjeta.

CSM_91 Una vez expedidas, las tarjetas de tacógrafo contendrán las siguientes claves criptográficas y certificados:

— La clave privada Card_MA y el certificado correspondiente.

— Además, en lo que se refiere a las tarjetas de conductor y las tarjetas de taller: la clave privada Card_Sign y el certificado correspondiente.

— El certificado MSCA_Card que contiene la clave pública MSCA_Card.PK que deberá utilizarse para la verificación del certificado Card_MA y el certificado Card_Sign.

— El certificado EUR que contiene la clave pública EUR.PK que deberá utilizarse para la verificación del certificado MSCA_Card.

— El certificado EUR cuyo período de validez es directamente anterior al período de validez del certificado EUR que deberá utilizarse para verificar el certificado MSCA_Card, si existe.

— El certificado de enlace que asocia estos dos certificados EUR, si existe.

CSM_92 Además de las claves criptográficas y los certificados enumerados en CSM_91, las tarjetas de tacógrafo deberán contener asimismo las claves y certificados especificados en la parte A del presente apéndice de forma que estas tarjetas puedan interactuar con las unidades instaladas en los vehículos de primera generación.

9.1.6 *Nivel de equipo: Dispositivos GNSS externos*

CSM_93 Para cada dispositivo GNSS externo se generará un par de claves ECC único designado EGF_MA. Esta tarea es efectuada por los fabricantes de dispositivos GNSS externos. Siempre que se genere un nuevo par de claves EGF_MA, la clave pública se enviará a a la MSCA del país en el que resida a fin de obtener el certificado EGF_MA correspondiente firmado por la MSCA. La clave privada será utilizada solamente por el dispositivo GNSS externo.

CSM_94 Un fabricante de EGF seleccionará la fortaleza de un par de claves EGF_MA igual a la fortaleza del par de claves MSCA utilizado para firmar el certificado correspondiente de EGF_MA.

CSM_95 Una dispositivo GNSS externo utilizará su par de claves EGF_MA, compuesto por la clave privada EGF_MA.SK y la clave pública EGF_MA.PK, exclusivamente para efectuar la autenticación mutua y establecer la clave de sesión con las unidades instaladas en los vehículos, tal como se especifica en las secciones 11.4 y 11.4 del presente apéndice.

CSM_96 El período de validez del certificado EGF_MA será de 15 años.

CSM_97 Un dispositivo GNSS externo no utilizará la clave privada de su par de claves EGF_MA para acoplarse con una unidad instalada en el vehículo una vez caducado el certificado correspondiente.

Nota: tal como se indica en la sección 11.3.3, una EGF puede potencialmente utilizar su clave privada para la autenticación mutua con la VU con la que ya esté acoplada, aun después de caducado el certificado correspondiente.

CSM_98 El par de claves EGF_MA y el certificado correspondiente de un dispositivo GNSS externo concreto no se sustituirán ni renovarán en el campo una vez puesta en funcionamiento la EGF.

Nota: Este requisito no prohíbe la posibilidad de sustituir pares de claves EGF durante una renovación o reparación en un entorno seguro controlado por el fabricante de la EGF.

CSM_99 Una vez puesta en funcionamiento, un dispositivo GNSS externo contendrá las siguientes claves criptográficas y certificados:

— La clave privada EGF_MA y el certificado correspondiente.

— El certificado MSCA_VU-EGF que contiene la clave pública MSCA_VU-EGF.PK que deberá utilizarse para la verificación del certificado EGF_MA.

— El certificado EUR que contiene la clave pública EUR.PK que deberá utilizarse para la verificación del certificado MSCA_VU-EGF.

— El certificado EUR cuyo período de validez es directamente anterior al período de validez del certificado EUR que deberá utilizarse para verificar el certificado MSCA_VU-EGF, si existe.

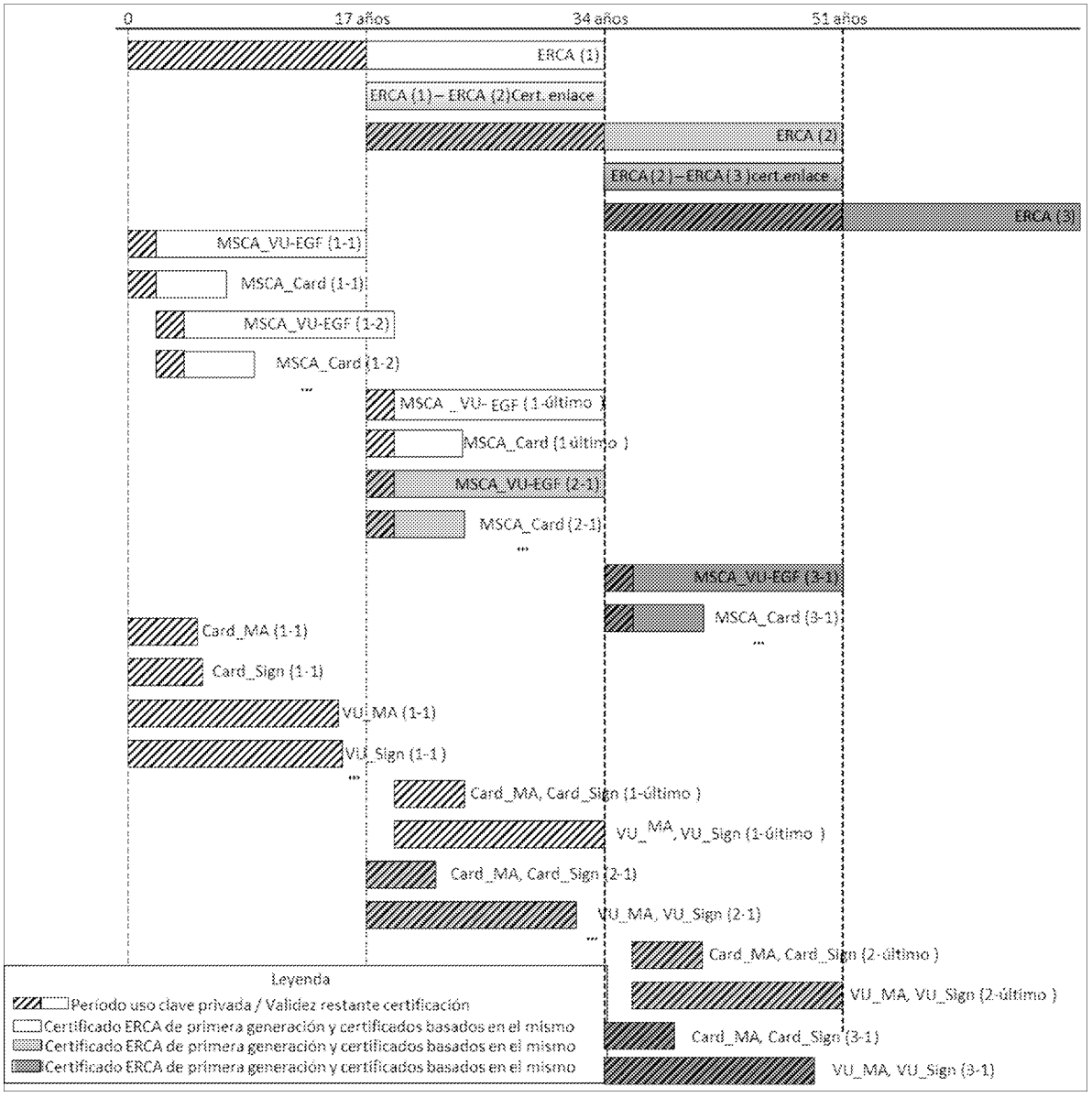
— El certificado de enlace que asocia estos dos certificados EUR, si existe.

9.1.7 *Síntesis: Sustitución del certificado*

La Figure 1 siguiente ilustra cronológicamente la forma en que se expiden y utilizan los certificados raíz ERCA, los certificados de enlace ERCA, los certificados MSCA y los certificados de equipos (VU y tarjeta):

Figura 1

Expedición y uso de las diferentes generaciones de certificados raíz ERCA, certificados de enlace ERCA, certificados MSCA y certificados de equipos



Notas de la Figure 1:

1. Las diferentes generaciones del certificado raíz se indican mediante un número entre paréntesis. Por ejemplo, ERCA (1) es la primera generación del certificado raíz ERCA; ERCA (2) es la segunda generación, etc.

2. Los demás certificados se indican mediante dos números entre paréntesis, el primero de los cuales indica la generación del certificado raíz correspondiente, y el segundo la generación del propio certificado. Por ejemplo, MSCA_Card (1-1) es el primer certificado MSCA_Card expedido en el marco del ERCA (1); MSCA_Card (2-1) es el primer certificado MSCA_Card expedido en el marco del ERCA (2); MSCA_Card (2-last) es el último certificado MSCA_Card expedido en el marco del ERCA (2); MSCA_Card (2-1) es el primer certificado para la autenticación mutua expedido en el marco del ERCA (2), etc.

3. Los certificados MSCA_Card (2-1) y MSCA_Card (1-last) son expedidos casi en la misma fecha, pero no exactamente. MSCA_Card (2-1) es el primer certificado MSCA_Card expedido en el marco del ERCA (2) y será expedido poco tiempo después que MSCA_Card (1-last), el último certificado MSCA_Card en el marco del ERCA (1).

4. Como indica la figura, los primeros certificados VU y Card expedidos en el marco del ERCA (2) aparecerán casi dos años antes de que aparezcan los últimos certificados VU y Card expedidos en el marco del ERCA (1). Esto es así porque los certificados VU y Card son expedidos en el marco de un certificado MSCA, y no directamente en el marco del certificado ERCA. El certificado MSCA (2-1) será expedido directamente después de que adquiera validez el ERCA (2), pero el certificado MSCA (1-last) será expedido solamente poco tiempo antes, en el último momento en que el certificado ERCA (1) es todavía válido. Por consiguiente, estos dos certificados MSCA tendrán casi el mismo período de validez, a pesar de que sean de dos generaciones diferentes.

5. El período de validez indicado para las tarjetas es el de las tarjetas de conductor (5 años).

6. Por limitaciones de espacio, solamente se indica la diferencia entre los períodos de validez de los certificados Card_MA y Card_Sign y entre los certificados VU_MA y VU_Sign de la primera generación.

9.2. **Claves simétricas**

9.2.1 *Claves de aseguramiento de la comunicación entre la VU y el sensor de movimiento*

9.2.1.1 *Generalidades*

Nota: se da por supuesto que los lectores de la presente sección están familiarizados con el contenido de la norma [ISO 16844-3] que describe la interfaz entre una unidad instalada en el vehículo y un sensor de movimiento. El proceso de emparejamiento entre una VU y un sensor de movimiento se describe en detalle en el capítulo 12 del presente apéndice.

CSM_100 Para aparear unidades instaladas en los vehículos y sensores de movimiento son necesarias varias claves simétricas a efectos de la autenticación mutua entre las unidades instaladas en los vehículos y los sensores de movimiento y del cifrado de la comunicación entre las unidades instaladas en los vehículos y los sensores de movimiento, como se indica en la Table 3. Todas estas claves serán claves AES, con una longitud de clave igual a la longitud de la clave maestra del sensor de movimiento, que estará relacionada con la longitud del par de claves raíz (previsto), tal como se describe en CSM_50.

Tabla 3

Claves de aseguramiento de la comunicación entre la unidad instalada en el vehículo y el sensor de movimiento

Clave	Símbolo	Generada por	Método de generación	Almacenada por
Clave maestra del sensor de movimiento — parte VU	$K_{M\text{-}VU}$	ERCA	Aleatorio	ERCA, MSCA implicadas en la expedición de certificados de VU, fabricantes de VU, unidades instaladas en los vehículos

Clave	Símbolo	Generada por	Método de generación	Almacenada por
Clave maestra del sensor de movimiento — parte taller	K_{M-WC}	ERCA	Aleatorio	ERCA, MSCA, fabricantes de tarjetas, tarjetas de taller
Clave maestra del sensor de movimiento	K_M	No generada independientemente	Calculada como $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, MSCA implicadas en la expedición de claves de sensores de movimiento (opcionalmente) (*)
Clave de identificación	K_{ID}	No generada independientemente	Calculada como $K_{ID} = K_M$ XOR CV, donde CV se especifica en CSM_106	ERCA, MSCA implicadas en la expedición de claves de sensores de movimiento (opcionalmente) (*)
Clave de emparejamiento	K_P	Fabricante del sensor de movimiento	Aleatorio	Un sensor de movimiento
Clave de sesión	K_S	VU (durante el emparejamiento de la VU y el sensor de movimiento)	Aleatorio	Una VU y un sensor de movimiento

(*) El almacenamiento de K_M y K_{ID} es optativo, ya que estas claves pueden derivarse de K_{M-VU}, K_{M-WC} y CV.

CSM_101 La Autoridad del Certificado Raíz Europeo generará K_{M-VU} yd K_{M-WC}, dos claves AES aleatorias y únicas a partir de las cuales la clave maestra del sensor de movimiento K_M se puede calcular como K_{M-VU} XOR K_{M-WC}. La ERCA comunicará previa solicitud las claves K_M, K_{M-VU} y K_{M-WC} a las autoridades de certificación de los Estados miembros.

CSM_102 La ERCA asignará a cada clave maestra de sensor de movimiento K_M un número de versión único, que será asimismo aplicable para las claves constitutivas K_{M-VU} y K_{M-WC} y para la clave de identificación asociada K_{ID}. La ERCA comunicará a las MSCA el número de versión al enviarles las claves K_{M-VU} y K_{M-WC}.

Nota: El número de versión se usa para distinguir generaciones diferentes de estas claves, como se explica en detalle en la sección 9.2.1.2.

CSM_103 Las autoridades de certificación de los Estados miembros remitirán previa solicitud la clave K_{M-VU}, junto con su número de versión, a los fabricantes de unidades instaladas en los vehículos. Los fabricantes de VU insertarán la clave K_{M-VU} y su número de versión en todas las VU fabricadas.

CSM_104 Las autoridades de certificación de los Estados miembros garantizarán que la clave K_{M-WC}, junto con su número de versión, sea insertada en cada tarjeta de taller expedida bajo su responsabilidad.

Notas:

— Véase la descripción del tipo de dato `SensorInstallationSecData` en el apéndice 2.

— Como se indica en la sección 9.2.1.2, de hecho puede ser necesario insertar múltiples generaciones de la clave K_{M-WC} en la misma tarjeta de taller.

CSM_105 Además de la clave AES especificada en CSM_104, las MSCA garantizarán que la clave Km_{WC} en TDES especificada en el requisito CSM_037 de la parte A del presente apéndice sea también insertada en cada tarjeta de taller expedida bajo su responsabilidad.

Notas:

— Esto permite utilizar una tarjeta de taller de segunda generación para emparejar una VU de primera generación.

— Una tarjeta de taller de segunda generación contendrá dos aplicaciones diferentes, una conforme con la parte B del presente apéndice y otra conforme con la parte A. Esta última contendrá la clave Km_{WC} en TDES.

CSM_106 Las MSCA implicadas en la expedición de sensores de movimiento derivarán la clave de identificación a partir de la clave maestra del sensor de movimiento aplicándole el operador XOR con un vector constante CV. El valor de CV será el siguiente:

— Para las claves maestras de sensor de movimiento de 128 bits: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83'

— Para las claves maestras de sensor de movimiento de 192 bits: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

— Para las claves maestras de sensor de movimiento de 256 bits: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Nota: los vectores constantes se han generado de la siguiente manera:

Pi_10 = primeros 10 bytes de la porción decimal de la constante matemática π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bits = primeros 16 bytes de SHA-256(Pi_10)

CV_192-bits = primeros 24 bytes de SHA-384(Pi_10)

CV_256-bits = primeros 32 bytes de SHA-512(Pi_10)

CSM_107 Los fabricantes de sensores de movimiento generarán una clave de emparejamiento K_P aleatoria y única para cada sensor de movimiento y enviarán cada clave de emparejamiento a la autoridad de certificación del Estado miembro. La MSCA cifrará cada clave de emparejamiento separadamente con la clave maestra K_M del sensor de movimiento y devolverá la clave cifrada al fabricante del sensor de movimiento. Para cada clave cifrada, la MSCA notificará al fabricante del sensor de movimiento el número de versión de la K_M asociada.

Nota: como se indica en la sección 9.2.1.2, de hecho puede ser necesario que un fabricante de sensores de movimiento tenga que generar claves de emparejamiento únicas múltiples para el mismo sensor de movimiento.

CSM_108 Los fabricantes de sensores de movimiento generarán un número de serie único para cada sensor de movimiento y enviarán todos los números de serie a la autoridad de certificación del Estado miembro. La MSCA cifrará cada número de serie separadamente con la clave de identificación maestra K_{ID} y devolverá el número de serie cifrado al fabricante del sensor de movimiento. Para cada número de serie cifrado, la MSCA notificará al fabricante del sensor de movimiento el número de versión de la K_{ID} asociada.

CSM_109 Para los requisitos CSM_107 y CSM_108, la MSCA utilizará el algoritmo AES in el modo de funcionamiento de cifrado progresivo por bloques, tal como se define en la norma [ISO 10116], con un parámetro interpolar m = 1 y un vector de inicialización SV = '00' {16}, es decir, dieciséis bytes con valor binario 0. Cuando sea necesario, la MSCA utilizará el método de relleno 2 definido en la norma [ISO 9797-1].

CSM_110 El fabricante del sensor de movimiento almacenará la clave de emparejamiento cifrada y el número de serie cifrado en el sensor de movimiento de que se trate, junto con los valores de texto sencillo correspondientes y el número de versión de las claves K_M y K_{ID} utilizadas para el cifrado.

Nota: como se indica en la sección 9.2.1.2, de hecho puede ser necesario que un fabricante de sensores de movimiento tenga que insertar múltiples claves de emparejamiento cifradas y múltiples números de serie cifrados en el mismo sensor de movimiento.

CSM_111 Además del material criptográfico basado en la norma AES especificado en CSM_110, puede ser necesario que un fabricante de sensores de movimiento tenga que almacenar asimismo en cada sensor de movimiento el material criptográfico en TDES especificado en el requisito CSM_037 de la parte A del presente apéndice.

Nota: esto permitirá que un sensor de movimiento de segunda generación pueda ser acoplado a una VU de primera generación.

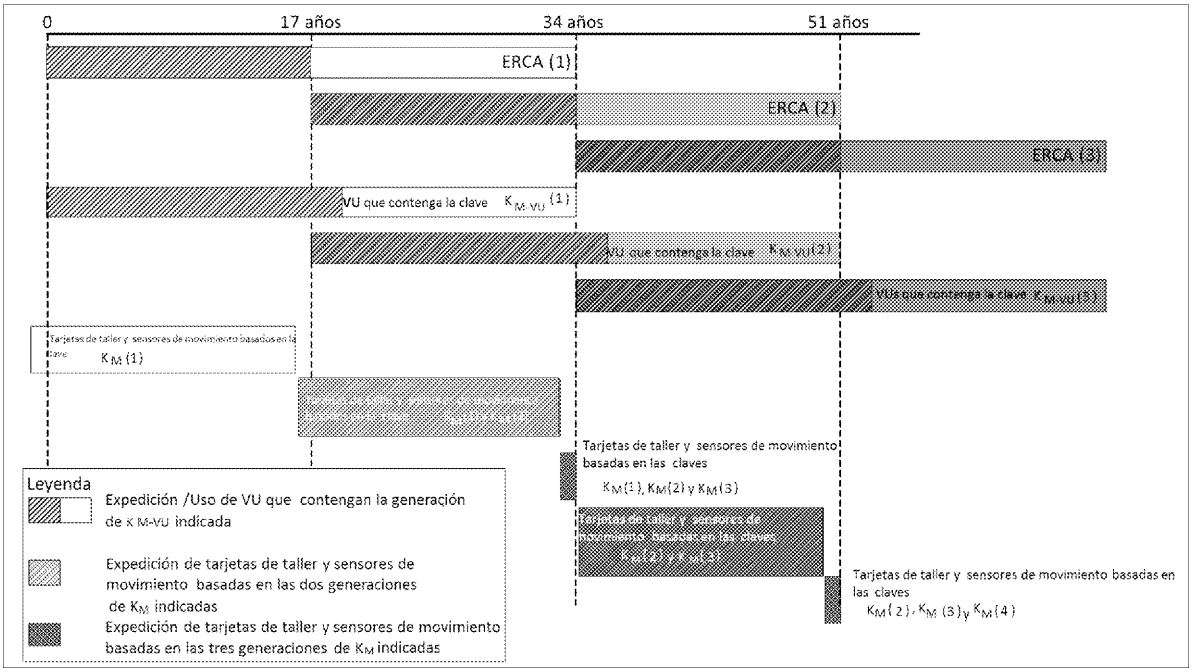
CSM_112 La longitud de la clave de sesión K_S generada por una VU durante el emparejamiento con un sensor de movimiento estará relacionada con la longitud de su K_{M-VU}, tal como se describe en CSM_50.

9.2.1.2 *Sustitución de la clave maestra del sensor de movimiento en los equipos de segunda generación*

CSM_113 Cada clave maestra del sensor de movimiento y todas las claves relacionadas (véase la Table 3) está asociada a una generación concreta del par de claves raíz de la ERCA. Estas claves se pueden por tanto sustituir cada 17 años. El período de validez de cada generación de clave maestra del sensor de movimiento comenzará un año antes de que adquiera validez el par de claves raíz de la ERCA asociado y finalizará cuando caduque el par de claves raíz de la ERCA asociado, tal como viene ilustrado en la Figure 2.

Figura 2

Expedición y uso de diferentes generaciones de la clave maestra del sensor de movimiento en las unidades instaladas en los vehículos, sensores de movimiento y tarjetas de taller



CSM_114 Al menos un año antes de generar un nuevo par de claves raíz europeo, tal como se describe en el punto CSM_56, la ERCA generará una nueva clave maestra del sensor de movimiento K_M generando las nuevas claves K_{M-VU} y K_{M-WC} La longitud de la clave maestra del sensor de movimiento estará relacionada con la longitud prevista del nuevo par de claves raíz europeo, de conformidad con el punto CSM_50. La ERCA comunicará, previa solicitud, las nuevas claves K_M, K_{M-VU} yd K_{M-WC}, junto con su número de versión, a las MSCA.

CSM_115 Las MSCA garantizarán que todas las generaciones válidas de la clave K_{M-WC} sean almacenadas en cada tarjeta de taller expedida bajo su autoridad, junto con su número de versión, tal como se indica en la Figure 2.

Nota: esto implica que durante el último año del período de validez de un certificado ERCA, las tarjetas de taller serán expedidas con tres generaciones diferentes de la clave K_{M-WC}, tal como se indica en la Figure 2.

CSM_116 En relación con el proceso descrito anteriormente en CSM_107 y CSM_108: Las MSCA cifrarán cada clave de emparejamiento K_P que reciban de un fabricante de sensores de movimiento separadamente con cada generación válida de la clave maestra del sensor de movimiento K_M. Las MSCA cifrarán asimismo cada número de serie que reciban de un fabricante de sensores de movimiento separadamente con cada generación válida de la clave de identificación K_{ID}. Los fabricantes de sensores de movimiento almacenarán todos los cifrados de la clave de emparejamiento y todos los cifrados del número de serie en el sensor de movimiento de que se trate, junto con los valores de texto sencillo correspondientes y el número o los números de versión de las claves K_M y K_{ID} utilizadas para el cifrado.

Nota: Esto implica que durante el último año del período de validez de un certificado ERCA, los sensores de movimiento serán expedidos con datos cifrados basados en tres generaciones diferentes de la clave K_M, tal como se indica en la Figure 2.

CSM_117 En relación con el proceso descrito anteriormente en CSM_107: Puesto que la longitud de la clave de emparejamiento K_P estará relacionada con la longitud de la clave K_M (véase CSM_100), es posible que un fabricante de sensores de movimiento tenga que generar hasta tres claves de emparejamiento diferentes (de diferentes longitudes) para un sensor de movimiento, para el caso en que generaciones posteriores de la clave K_M tengan longitudes diferentes. En tal caso, el fabricante enviará cada clave de emparejamiento a la MSCA. La MSCA garantizará que cada clave de emparejamiento sea cifrada con la generación correcta de la clave maestra del sensor de movimiento, es decir, con la que tenga la misma longitud.

Nota: En el caso de que el fabricante de sensores de movimiento opte por generar en TDES una clave de emparejamiento para un sensor de movimiento de segunda generación (véase CSM_111), el fabricante indicará a la MSCA que para cifrar esta clave de emparejamiento debe emplearse la clave maestra en TDES del sensor de movimiento. Esto es así porque la longitud de una clave TDES puede ser igual a la de una clave AES, de forma que la MSCA no puede distinguir una de la otra solamente por la longitud de la clave.

CSM_118 Los fabricantes de unidades instaladas en los vehículos insertarán solamente una generación de la clave K_{M-VU} en cada unidad instalada en el vehículo, junto con su número de versión. Esta generación de clave K_{M-VU} estará relacionada con el certificado de la ERCA en que se basen los certificados de la UV.

Notas:

— Una unidad instalada en el vehículo basada en el certificado ERCA de generación X solamente deberá contener la clave K_{M-VU} de generación X aun en el caso de que sea expedida después del inicio del período de validez del certificado ERCA de generación X+1. Esto viene ilustrado en la Figure 2.

— Una VU de generación X no puede emparejarse con un sensor de movimiento de generación X-1.

— Puesto que las tarjetas de taller tienen un período de validez de un año, el resultado de CSM_113 — CSM_118 es que todas las tarjetas de taller contendrán la nueva clave K_{M-WC} en el momento en que sea expedida la primera VU que contenga la nueva clave K_{M-VU}. Por consiguiente, esa VU siempre podrá calcular la nueva clave $K_{M.}$. Además, para entonces la mayoría de los sensores de movimiento nuevos contendrán datos cifrados también basados en la nueva clave $K_{M.}$.

9.2.2 *Claves de aseguramiento de comunicaciones dedicadas de corto alcance (DSRC)*

9.2.2.1 *Generalidades*

CSM_119 La autenticidad y confidencialidad de los datos comunicados desde una unidad instalada en el vehículo a una autoridad de control a través de un canal de comunicación remota DSRC se asegurará mediante una serie de claves AES específicas de la VU derivadas de una única clave maestra de DSRC, KM_{DSRC}.

CSM_120 La clave maestra de DSRC KM_{DSRC} será una clave AES generada, almacenada y distribuida de forma segura por la ERCA. La longitud de la clave será de 128, 192 o 256 bits y estará relacionada con la longitud del par de claves raíz europeo, tal como se describe en CSM_50.

CSM_121 La ERCA comunicará previa solicitud la clave maestra DSRC a las autoridades de certificación de los Estados miembros de forma segura a fin de permitirles derivar claves DSRC específicas de las VU y asegurar que la clave maestra DSRC sea insertada en todas las tarjetas de control y tarjetas de taller expedidas bajo su responsabilidad.

CSM_122 La ERCA asignará a cada clave maestra DSRC un número de versión único. La ERCA comunicará a las MSCA el número de versión al enviarles la clave maestra DSRC.

Nota: El número de versión se usa para distinguir generaciones diferentes de la clave maestra DSRC, como se explica en detalle en la sección 9.2.2.2.

CSM_123 Para cada unidad instalada en el vehículo, el fabricante de la unidad instalada en el vehículo creará un número de serie de la UV único y lo enviará a la autoridad de certificación de su Estado miembro en una solicitud de obtención de un conjunto de dos claves DSRC específicas de la VU. El número de serie de la VU tendrá el tipo de dato `VuSerialNumber`, y para el cifrado se utilizarán las reglas de codificación distinguida (DER) según la norma [ISO 8825-1].

CSM_124 Cuando reciba una solicitud de claves DSRC específicas de una VU, la MSCA derivará dos claves AES para la unidad instalada en el vehículo, denominadas K_VU_{DSRC}_ENC y K_VU_{DSRC}_MAC. Estas claves específicas de la VU tendrán la misma longitud que la clave maestra DSRC. La MSCA utilizará la función de derivación de claves definida en el documento [RFC 5869]. La función resumen (o función hash) necesaria para instanciar la función HMAC-Hash estará relacionada con la longitud de la clave maestra DSRC, tal como se describe en CSM_50. La función de derivación de la clave que figura en el documento [RFC 5869] se utilizará del siguiente modo:

Paso 1 (Extraer):

— *PRK* = HMAC-Hash (*salt, IKM*) donde *salt* es una cadena vacía '' e *IKM* es KM_{DSRC}.

Paso 2 (Expandir):

— *OKM* = *T(1)*, donde

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || '01') con

— *T(0)* = una cadena vacía ('')

— *info* = número de serie de la VU tal como se especifica en CSM_123

— K_VU_{DSRC}_ENC = primeros octetos *L* de *OKM* y

K_VU_{DSRC}_MAC = últimos octetos *L* de *OKM*

donde *L* es la longitud requerida de K_VU_{DSRC}_ENC y K_VU_{DSRC}_MAC en octetos.

CSM_125 La MSCA distribuirá las claves K_VU_{DSRC}_ENC y K_VU_{DSRC}_MAC al fabricante de VU de forma segura para su inserción en la unidad instalada en el vehículo de que se trate.

CSM_126 Una vez expedida, una unidad instalada en el vehículo llevará almacenadas las claves K_VU_{DSRC}_ENC y K_VU_{DSRC}_MAC en su memoria protegida a fin de poder garantizar la integridad, autenticidad y confidencialidad de los datos enviados por el canal de comunicación remota. Una unidad instalada en el vehículo también llevará almacenado el número de versión de la clave maestra DSRC utilizada para derivar estas claves específicas de la VU.

CSM_127 Una vez expedidas, las tarjetas de control y las tarjetas de taller llevarán almacenada la clave KM_{DSRC} en su memoria protegida a fin de poder verificar la integridad y autenticidad de los datos enviados por una VU por un canal de comunicación remota y de descifrar estos datos. Las tarjetas de control y las tarjetas de taller también llevarán almacenado el número de versión de la clave maestra DSRC.

Nota: Como se indica en la sección 9.2.2.2, de hecho puede ser necesario insertar múltiples generaciones de la clave KM_{DSRC} en la misma tarjeta de taller o tarjeta de control.

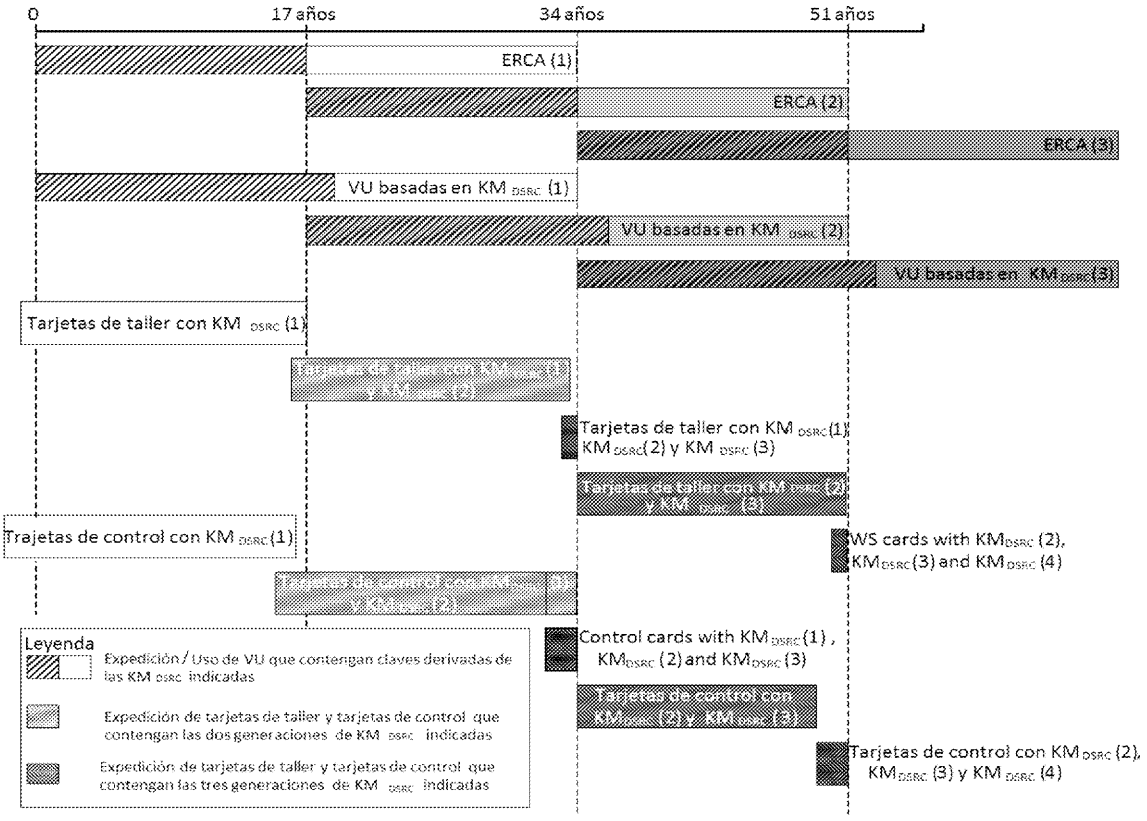
CSM_128 La MSCA llevará un registro de todas las claves DSRC específicas de VU que haya generado, su número de versión y la identificación de las VU a las que se haya destinado cada conjunto de claves.

9.2.2.2 *Sustitución de la clave maestra DSRC*

CSM_129 Cada clave maestra DSRC está asociada a una generación concreta del par de claves raíz de la ERCA. Por consiguiente, la ERCA sustituirá la clave maestra DSRC dada 17 años. El período de validez de cada generación de clave maestra DSRC comenzará dos años antes de que adquiera validez el par de claves raíz de la ERCA asociado y finalizará cuando caduque el par de claves raíz de la ERCA asociado, tal como se ilustra en la Figure 3.

Figura 3

Expedición y uso de diferentes generaciones de la clave maestra DSRC en las unidades instaladas en los vehículos, tarjetas de taller y tarjetas de control



CSM_130 Al menos un año antes de generar un nuevo par de claves raíz europeo, tal como se describe en el punto CSM_56, la ERCA generará una nueva clave maestra DSRC. La longitud de la clave maestra DSRC estará relacionada con la longitud prevista del nuevo par de claves raíz europeo, de conformidad con el punto CSM_50. La ERCA comunicará, previa solicitud, la nueva clave DSRC, junto con su número de versión, a las MSCA.

CSM_131 Las MSCA garantizarán que todas las generaciones válidas de la clave KM_{DSRC} sean almacenadas en cada tarjeta de control expedida bajo su autoridad, junto con sus números de versión, tal como se indica en la Figure 2.

Nota: esto implica que durante los dos últimos años del período de validez de un certificado ERCA, las tarjetas de control serán expedidas con tres generaciones diferentes de la clave KM_{DSRC}, tal como se indica en la Figure 2.

CSM_132 Las MSCA garantizarán que todas las generaciones de la clave KM_{DSRC} que hayan sido válidas durante al menos un año sean almacenadas en cada tarjeta de control expedida bajo su autoridad, junto con sus números de versión, tal como se indica en la Figure 2.

Nota: esto implica que durante el último año del período de validez de un certificado ERCA, las tarjetas de taller serán expedidas con tres generaciones diferentes de la clave KM_{DSRC}, tal como se indica en la Figure 2.

CSM_133 Los fabricantes de unidades instaladas en los vehículos insertarán solamente un conjunto de claves DSRC específicas de la VU en cada unidad instalada en el vehículo, junto con su número de versión. Este conjunto de claves se derivará de la generación de la KM_{DSRC} relacionada con el certificado de la ERCA en que se basen los certificados de la VU.

Notas:

— Esto implica que una unidad instalada en el vehículo basada en el certificado ERCA de la generación X solamente deberá contener las claves K_VU_{DSRC}_ENC K_{M-VU} y K_VU_{DSRC}_MAC de la generación X, aun en el caso de que la VU sea expedida después del inicio del período de validez del certificado ERCA de la generación X+1., tal como se indica en la Figure 3.

— Puesto que las tarjetas de taller tienen un período de validez de un año y las tarjetas de control de dos años, el resultado de CSM_131 — CSM_133 es que todas las tarjetas de taller y tarjetas de control contendrán la nueva clave maestra DSRC en el momento en que sea expedida la primera VU que contenga claves específicas de la VU basadas en esa clave maestra.

9.3. **Certificados**

9.3.1 *Generalidades*

CSM_134 Todos los certificados del sistema europeo de tacógrafo inteligente serán certificados autodescriptivos y verificables con tarjeta (CV) de acuerdo con las normas [ISO 7816-4] y [ISO 7816-8].

CSM_135 A fin de codificar tanto las estructuras de datos ASN.1 como los objetos de datos (específicos de las aplicaciones) en los certificados, se utilizarán las reglas de codificación distinguida (DER) de acuerdo con la norma [ISO 8825-1].

Nota: esta codificación resulta en una estructura etiqueta-longitud-valor (TLV) como la siguiente:

Etiqueta: La etiqueta está codificada en uno o dos octetos e indica el contenido.

Longitud: La longitud está codificada como un número entero no firmado en uno, dos, o tres octetos, que resultan en una longitud máxima de 65 535 octetos. Se utilizará el número de octetos mínimo.

Valor: El valor está codificado en cero o más octetos.

9.3.2 *Contenido de los certificados*

CSM_136 Todos los certificados tendrá la estructura indicada en el perfil de certificado de la Table 4.

Tabla 4

Perfil de certificado versión 1

Campo	ID del campo	Etiqueta	Longitud (bytes)	Tipo de dato ASN.1 (véase el apéndice 1)
Certificado ECC	C	'7F 21'	var	
Organismo de certificación ECC	B	'7F 4E'	var	

Campo	ID del campo	Etiqueta	Longitud (bytes)	Tipo de dato ASN.1 (véase el apéndice 1)
Identificador del perfil de certificado	CPI	'5F 29'	'01'	INTEGER(0..255)
Referencia de la autoridad de certificación	CAR	'42'	'08'	KeyIdentifier
Autorización del titular del certificado	CHA	'5F 4C'	'07'	CertificateHolder Authorisation
Clave pública	PK	'7F 49'	var	
Parámetros de dominio	DP	'06'	var	OBJECT IDENTIFIER
Punto público	PP	'86'	var	OCTET STRING
Referencia al titular del certificado	CHR	'5F 20'	'08'	KeyIdentifier
Fecha efectiva del certificado	CEfD	'5F 25'	'04'	TimeReal
Fecha de caducidad del certificado	CExD	'5F 24'	'04'	TimeReal
Firma del certificado ECC	S	'5F 37'	var	OCTET STRING

Nota: el ID del campo se utilizará más adelante en otras secciones del presente apéndice para indicar campos individuales de un certificado, por ejemplo, X.CAR es la referencia de la autoridad de certificación mencionada en el certificado del usuario X.

9.3.2.1 Identificador del perfil de certificado

CSM_137 Los certificados utilizarán un identificador del perfil de certificado para indicar el perfil de certificado utilizado. La versión 1, tal como se especifica en la Table 4, se identificará con el valor '00'.

9.3.2.2 Referencia de la autoridad de certificación

CSM_138 La referencia de la autoridad de certificación se utilizará para identificar la clave pública que se deberá utilizar para verificar la firma del certificado. La referencia de la autoridad de certificación será por tanto igual a la referencia del titular del certificado en el certificado de la autoridad de certificación correspondiente.

CSM_139 Un certificado raíz de la ERCA estará autofirmado, es decir, la referencia en el certificado de la autoridad de certificación y del titular del certificado serán iguales.

CSM_140 Para un certificado de enlace ERCA, la referencia del titular del certificado será igual a la CHR del nuevo certificado raíz de la ERCA. La referencia de la autoridad de certificación para un certificado de enlace será igual a la CHR del certificado raíz ERCA anterior.

9.3.2.3 Autorización del titular del certificado (CHA)

CSM_141 La autorización del titular del certificado servirá para identificar el tipo de certificado. Se compone de los seis bytes más significativos del identificador de la aplicación del tacógrafo, concatenados con el tipo de equipo al que está destinado el certificado.

9.3.2.4 Clave pública

La clave pública anida dos elementos de datos: los parámetros de dominio normalizados que deberán utilizarse con la clave pública en el certificado y el valor del punto público.

CSM_142 El elemento de datos Domain Parameters contendrá uno de los identificadores de objeto especificados en la Table 1 para referenciar un conjunto de parámetros de dominio normalizados.

CSM_143 El elemento de datos Public Point contendrá el punto público. Los puntos públicos de curva elíptica se convertirán en cadenas de octetos tal como se especifica en la directriz técnica [TR-03111]. Se utilizará el formato de codificación descomprimido. Al recuperar un punto de curva elíptica de su formato codificado, siempre se efectuarán las validaciones descritas en la directriz técnica [TR-03111].

9.3.2.5 Referencia del titular del certificado (CHR)

CSM_144 La referencia del titular del certificado es un identificador de la clave pública indicado en el certificado. Se utilizará para referenciar esta clave pública en otros certificados.

CSM_145 Para los certificados de tarjeta y los certificados de dispositivo GNSS externo, la referencia del titular del certificado tendrá el tipo de dato `ExtendedSerialNumber` especificado en el apéndice 1.

CSM_146 En relación con las unidades instaladas en los vehículos, al solicitar un certificado, el fabricante puede conocer, o bien desconocer, el número de serie específico del fabricante de la VU a la que vayan destinados el certificado y la clave privada asociada. En el primer caso, la referencia del titular del certificado tendrá el tipo de dato `ExtendedSerialNumber` especificado en el apéndice 1. En el segundo caso, la referencia del titular del certificado tendrá el tipo de dato `CertificateRequestID` especificado en el apéndice 1.

CSM_147 En relación con los certificados ERCA y MSCA, la referencia del titular del certificado tendrá el tipo de dato `CertificationAuthorityKID` especificado en el apéndice 1.

9.3.2.6 Fecha efectiva del certificado

CSM_148 La fecha efectiva del certificado indicará la fecha y hora de inicio del período de validez del certificado. La fecha efectiva del certificado será la fecha de generación del certificado.

9.3.2.7 Fecha de caducidad del certificado

CSM_149 La fecha efectiva de caducidad del certificado indicará la fecha y hora de finalización del período de validez del certificado.

9.3.2.8 Firma del certificado

CSM_150 La firma del certificado se creará a través del contenido codificado del certificado, incluidas la etiqueta y la longitud del contenido del certificado. El algoritmo de firma será ECDSA, tal como se especifica en la norma [DSS], utilizando el algoritmo hash relacionado con el tamaño de la clave de la autoridad firmante, tal como se especifica en CSM_50. El formato de la firma será de texto plano, tal como se especifica en la directriz técnica [TR-03111].

9.3.3 *Solicitud de certificados*

CSM_151 Al solicitar un certificado, el solicitante enviará los siguientes datos a su autoridad de certificación:

— el identificador del perfil de certificado del certificado solicitado

— la referencia de la autoridad de certificación prevista para la firma del certificado

— la clave pública que deba firmarse

CSM_152 Además de los datos indicados en CSM_151, en una solicitud de certificado las MSCA enviarán los siguientes datos a la ERCA a fin de permitirle crear la referencia del titular del certificado de nuevo certificado MSCA:

— el código numérico del país de la autoridad de certificación (tipo de dato `NationNumeric` definido en el apéndice 1)

— el código alfanumérico del país de la autoridad de certificación (tipo de dato `NationAlpha` definido en el apéndice 1)

— el número de serie de 1 byte para distinguir las diferentes claves de la autoridad de certificación en caso de que se cambien las claves

— el campo de dos bytes que contiene la información adicional específica de la autoridad de certificación

CSM_153 Además de los datos indicados en CSM_151, en una solicitud de certificado los fabricantes de equipos enviarán los siguientes datos a la MSCA a fin de permitirle crear la referencia del titular del certificado del nuevo certificado de equipo:

— un identificador específico del fabricante del tipo de equipo

— si se conoce (véase CSM_154), un número de serie para el equipo, único para el fabricante, el tipo de equipo, y el mes de fabricación. En caso contrario, un identificador único de la solicitud de certificado.

— El mes y año de fabricación del equipo o de solicitud del certificado.

El fabricante garantizará que estos datos sean correctos y que el certificado devuelto por la MSCA sea insertado en el equipo previsto.

CSM_154 En el caso de una VU, al solicitar un certificado, el fabricante puede conocer, o bien desconocer, el número de serie específico del fabricante de la VU a la que vayan destinados el certificado y la clave privada asociada. Si lo conoce, el fabricante de VU enviará el número de serie a la MSCA. Si no lo conoce, el fabricante identificará de forma unívoca cada solicitud de certificado y enviará este número de serie de solicitud de certificado a la MSCA. El certificado resultante contendrá el número de serie de la solicitud de certificado. Una vez insertado el certificado en una VU específica, el fabricante comunicará la conexión entre el número de serie de la solicitud de certificado y la identificación de la VU a la MSCA.

10. AUTENTICACIÓN MUTUA DE LA TARJETA VU_CARD Y MENSAJERÍA SEGURA

10.1. **Generalidades**

CSM_155 A un nivel elevado, la comunicación segura entre una unidad instalada en el vehículo y una tarjeta de tacógrafo se basará en los siguientes pasos:

— En primer lugar, cada parte demostrará a la otra que detenta un certificado de clave pública válido y firmado por una autoridad de certificación de un Estado miembro. A su vez, el certificado de clave pública MSCA debe estar firmado por la Autoridad del Certificado Raíz Europeo. Este paso se denomina verificación de la cadena de certificados y se especifica en detalle en la sección 10.2

— En segundo lugar, la unidad instalada en el vehículo demostrará a la tarjeta que está en posesión de la clave privada que corresponde a la clave pública en el certificado presentado firmando un número aleatorio enviado por la tarjeta. La tarjeta verifica la firma a través del número aleatorio. Si la verificación se efectúa correctamente, se autentica la VU. Este paso se denomina autenticación de la VU y se especifica en detalle en la sección 10.3

— En tercer lugar, ambas partes calculan por separado dos claves de sesión AES utilizando un algoritmo de cifrado asimétrico. Usando una de estas claves de sesión, la tarjeta crea un código de autenticación de mensaje (MAC) a través de datos enviados por la VU. La VU verifica el MAC. Si la verificación se efectúa correctamente, se autentica la tarjeta. Este paso se denomina autenticación de la tarjeta y se especifica en detalle en la sección 10.4

— En cuarto lugar, la VU y la tarjeta usarán las claves de sesión acordadas para asegurar la confidencialidad, integridad y autenticidad de todos los mensajes intercambiados. Esto se denomina mensajería segura y se especifica en detalle en la sección 10.5

CSM_156 El mecanismo descrito en CSM_155 será desencadenado por la unidad del vehículo siempre que se inserte una tarjeta en una de sus ranuras para tarjeta.

10.2. **Verificación mutua de la cadena de certificados**

10.2.1 *Verificación por la VU de la cadena de certificados de una tarjeta*

CSM_157 Las unidades instaladas en el vehículo utilizarán el protocolo ilustrado en la Figure 4 para verificar la cadena de certificados de una tarjeta de tacógrafo.

Notas de la Figure 4:

— Los certificados de tarjeta y las claves públicas mencionados en la figura son los empleados para la autenticación mutua. La sección 9.1.5 los denota Card_MA.

— Los certificados Card.CA y las claves públicas mencionados en la figura son los empleados para firmar los certificados de tarjeta y están indicados en la referencia CAR del certificado Card. La sección 9.1.3 los denota MSCA_Card.

— El certificado Card.CA.EUR mencionado en la figura es el certificado raíz europeo indicado en la referencia CAR del certificado Card.CA.

— El certificado Card.Link mencionado en la figura es el certificado de enlace de la tarjeta, si está presente. Tal como se especifica en la sección 9.1.2, este es el certificado de enlace para un nuevo par de claves raíz europeo creado por la ERCA y firmado por la clave privada europea anterior.

— El certificado Card.Link.EUR es el certificado raíz europeo indicado en la referencia CAR del certificado Card.Link.

CSM_158 Tal como ilustra la Figure 4, la verificación de la cadena de certificados de la tarjeta se iniciará al insertar la tarjeta. La unidad instalada en el vehículo leerá la referencia del titular de la tarjeta (`cardExtendedSerialNumber`) del número de serie de la EF.ICC. La VU comprobará si conoce la tarjeta, es decir, si ha verificado correctamente la cadena de certificados de la tarjeta en el pasado y la ha almacenado para futuras referencias. Si la conoce y el certificado de la tarjeta es todavía válido, el proceso continúa con la verificación de la cadena de certificados de la VU. De otro modo, la VU leerá sucesivamente en la tarjeta el certificado MSCA_Card que deberá utilizarse para verificar el certificado de la tarjeta, el certificado Card.CA.EUR necesario para verificar el certificado MSCA_Card y, posiblemente, el certificado de enlace, hasta que encuentre un certificado que conozca o pueda verificar. Si encuentra dicho certificado, la VU lo utilizará para verificar los certificados de tarjeta subyacentes que ha leído en la tarjeta. Si la verificación es correcta, el proceso continúa con la verificación de la cadena del certificado de la VU. Si no puede efectuarse la verificación, la VU ignorará la tarjeta.

Nota: La VU puede conocer el certificado Card.CA.EUR de tres maneras:

— el certificado Card.CA.EUR es el mismo certificado que el propio certificado EUR de la VU;

— el certificado Card.CA.EUR precede al propio certificado EUR de la VU, y la VU ya contenía este certificado en el momento de su expedición (véase CSM_81);

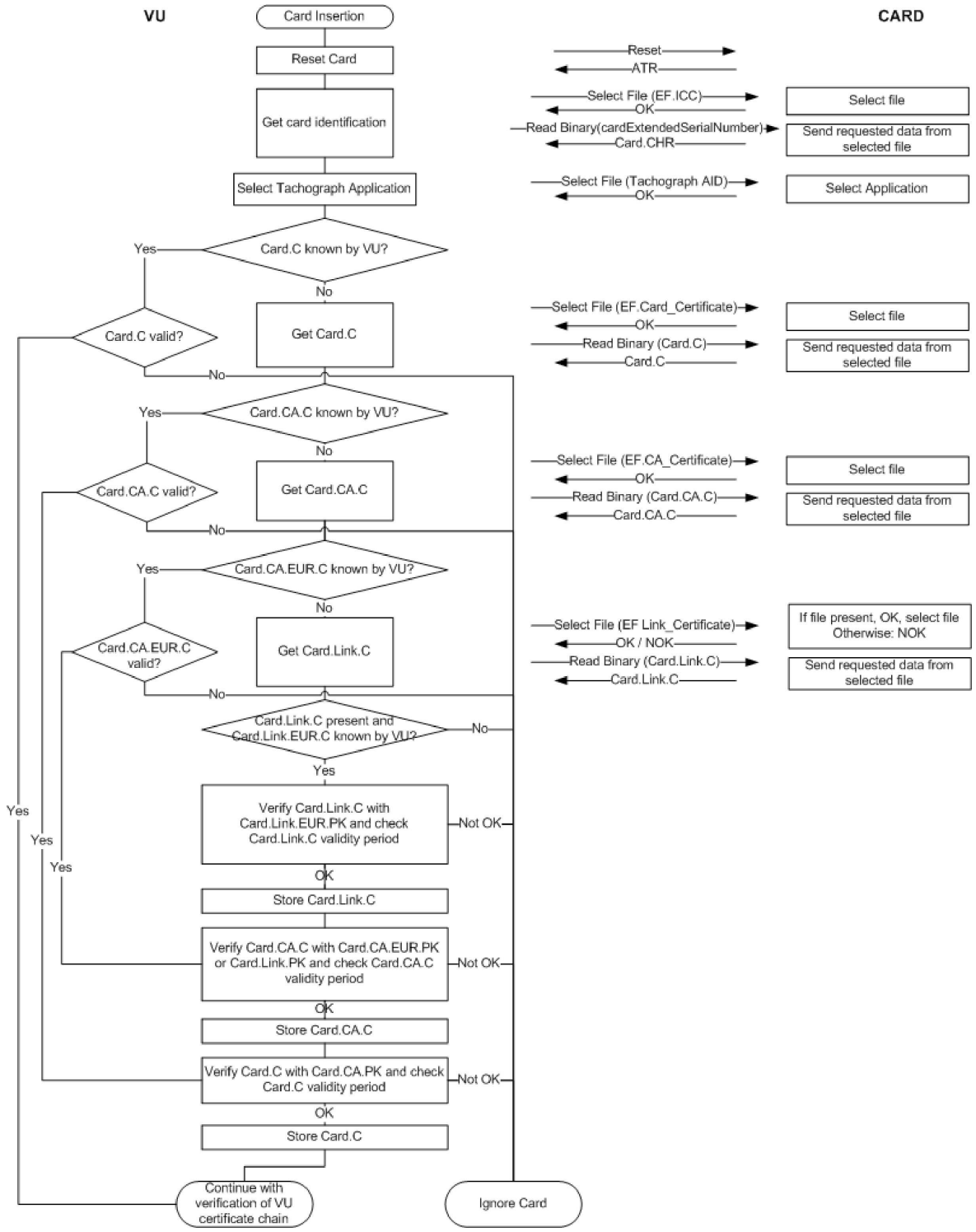
— el certificado Card.CA.EUR sucede al propio certificado EUR de la VU y la VU recibió un certificado de enlace en algún momento de otra tarjeta de tacógrafo, la verificó y la almacenó para referencias futuras.

CSM_159 Como se indica en la Figure 4, una vez que la VU ha verificado la autenticidad y validez de un certificado previamente desconocido, puede almacenar este certificado para referencias futuras, de modo que no tenga que volver a verificar la autenticidad del certificado si se vuelve a presentar a la VU. En lugar de almacenar la totalidad del certificado, una VU puede optar por almacenar solamente el contenido del certificado, tal como se especifica en la sección 9.3.2.

CSM_160 La VU verificará la validez temporal de todos los certificados leídos en la tarjeta o almacenados en su memoria, y rechazará los certificados caducados. Para verificar la validez temporal de un certificado presentado por la tarjeta, la VU utilizará su reloj interno.

Figura 4

Protocolo para la verificación de la cadena de certificados de una tarjeta por la VU

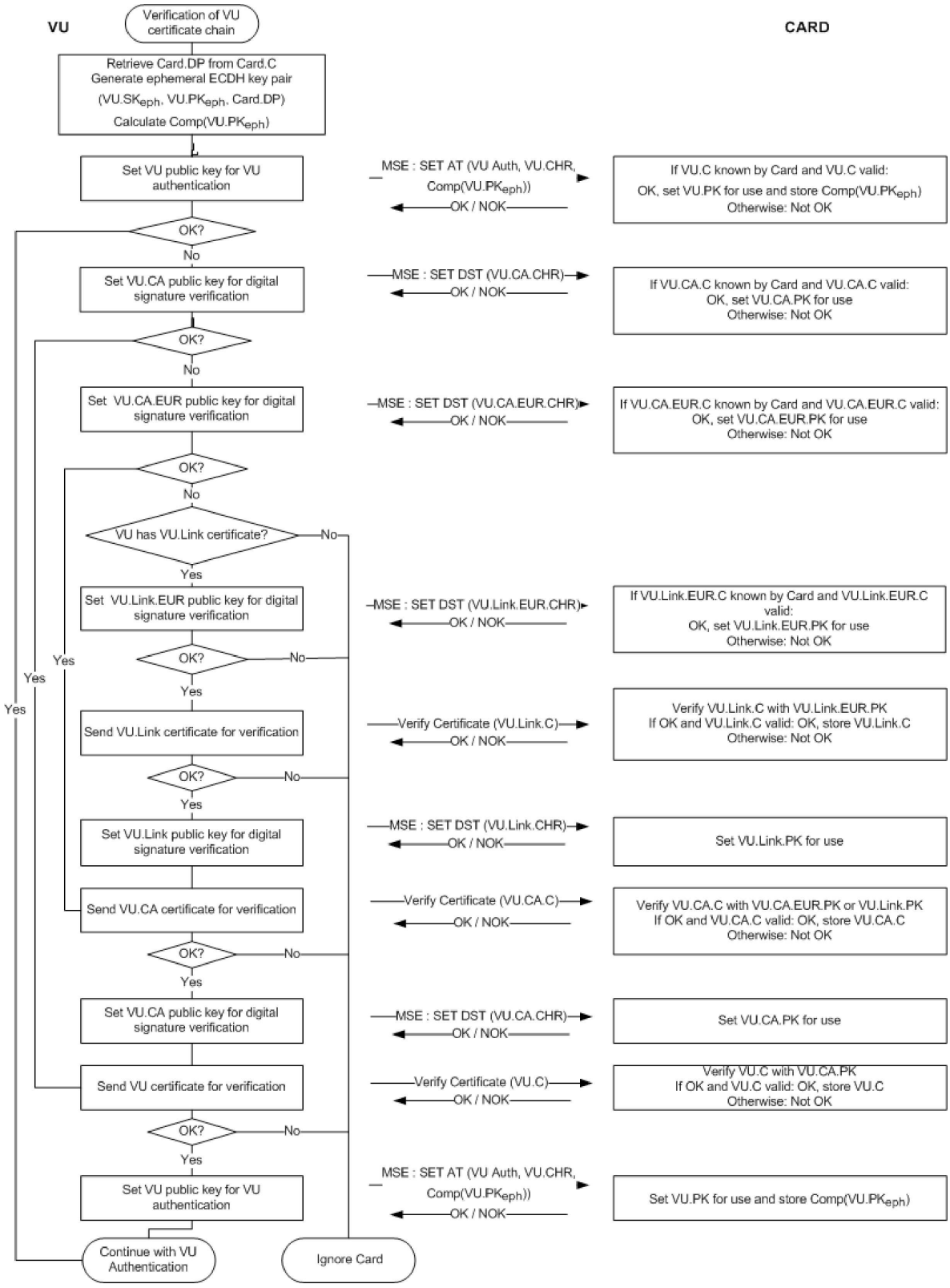


10.2.2 *Verificación por la tarjeta de la cadena de certificados de una VU*

CSM_161 Las tarjetas de tacógrafo utilizarán el protocolo ilustrado en la Figure 5 para verificar la cadena de certificados de una VU.

Figura 5

Protocolo para la verificación por una tarjeta de la cadena de certificados de una VU



Notas de la Figure 5:

— Los certificados de VU y las claves públicas mencionados en la figura son los empleados para la autenticación mutua. La sección 9.1.4 los denota VU_MA.

— Los certificados VU.CA y las claves públicas mencionados en la figura son los empleados para firmar los certificados de VU y de dispositivo GNSS externo. La sección 9.1.3 los denota MSCA_VU-EGF.

— El certificado VU.CA.EUR mencionado en la figura es el certificado raíz europeo indicado en la referencia CAR del certificado VU.CA.

— El certificado VU.Link mencionado en la figura es el certificado de enlace de la VU, si está presente. Tal como se especifica en la sección 9.1.2, este es el certificado de enlace para un nuevo par de claves raíz europeo creado por la ERCA y firmado por la clave privada europea anterior.

— El certificado VU.Link.EUR es el certificado raíz europeo indicado en la referencia CAR del certificado VU. Link.

CSM_162 Como ilustra la Figure 5, la verificación de la cadena de certificados de la unidad instalada en el vehículo se iniciará cuando esta intente establecer su propia clave pública para su uso en la tarjeta de tacógrafo. Si esto se efectúa correctamente, significa que la tarjeta ha verificado con éxito anteriormente la cadena de certificados de la VU y ha almacenado el certificado VU para referencias futuras. En este caso, el certificado VU está listo para usar y el proceso continúa con la autenticación de la VU. Si la tarjeta no conoce el certificado de la VU, la VU presentará sucesivamente el certificado MSCA_VU necesario para verificar el certificado de la VU, el certificado VU. CA.EUR necesario para verificar el certificado MSCA_VU y, posiblemente, el certificado de enlace, hasta encontrar un certificado conocido o verificable por la tarjeta. Si encuentra dicho certificado, la tarjeta lo utilizará para verificar los certificados VU subyacentes que le sean presentados. Si la verificación se efectúa correctamente, la VU establecerá finalmente su clave pública para uso en la tarjeta de tacógrafo. Si no puede efectuarse la verificación, la VU ignorará la tarjeta.

Nota: La tarjeta puede conocer el certificado VU.CA.EUR de tres maneras:

— el certificado VU.CA.EUR es el mismo certificado que el propio certificado EUR de la tarjeta;

— el certificado VU.CA.EUR precede al propio certificado EUR de la tarjeta, y la tarjeta ya contenía este certificado en el momento de su expedición (véase CSM_81);

— el certificado VU.CA.EUR sucede al propio certificado EUR de la tarjeta y la tarjeta recibió un certificado de enlace en algún momento de otra unidad instalada en el vehículo, la verificó y la almacenó para referencias futuras.

CSM_163 La VU utilizará el comando MSE (Message Security Environment): Set AT para establecer su clave pública para uso en la tarjeta de tacógrafo. Como se especifica en el apéndice 2, este comando contiene una indicación del mecanismo criptográfico que se utilizará con la clave establecida. Este mecanismo será 'Autenticación de VU mediante el algoritmo ECDSA, en combinación con el algoritmo hash relacionado con el tamaño de clave del par de claves VU_MA de la VU, tal como se especifica en CSM_50'.

CSM_164 El comando MSE: Set AT también contiene una indicación del par de claves efímero que la VU utilizará durante el acuerdo de claves de sesión (véase la sección 10.4). Por tanto, antes de enviar el comando MSE: Set AT, la VU generará un par de claves ECC efímero. Para generar el par de claves efímero, la VU utilizará los parámetros de dominio normalizados indicados en el certificado de la tarjeta. El par de claves efímero se denota por ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). La VU considerará la coordenada x del punto público efímero ECDH como la identificación de la clave; esto se denomina la representación comprimida de la clave pública y se denota por Comp($VU.PK_{eph}$).

CSM_165 Si el comando MSE: Set AT se ejecuta correctamente, la tarjeta establecerá la VU.PK indicada para su uso posterior durante la autenticación del vehículo, y almacenará temporalmente Comp(VU. PK_{eph}). En el caso de que se envíen dos o más comandos MSE: Set AT ejecutados correctamente antes de efectuar el acuerdo de claves de sesión, la tarjeta almacenará únicamente la última Comp ($VU.PK_{eph}$) recibida.

CSM_166 La tarjeta verificará la validez temporal de todos los certificados presentados por la VU o referenciados por la VU mientras están almacenados en la memoria de la tarjeta, y rechazará los certificados caducados.

CSM_167 Para verificar la validez temporal de un certificado presentado por la VU, cada tarjeta de tacógrafo almacenará internamente datos que representen la hora actual. Estos datos no serán directamente actualizables por una VU. En el momento de su expedición, la hora actual de una tarjeta que se configurará será la misma que la fecha efectiva del certificado Card_MA de la tarjeta. Una tarjeta actualizará su hora actual si la fecha efectiva de un certificado auténtico de 'fuente válida de hora' presentado por una VU es más reciente que la hora actual de la tarjeta. En tal caso, la tarjeta configurará su hora actual a la fecha efectiva de ese certificado. La tarjeta solamente aceptará los certificados siguientes como fuente válida de hora:

— Certificados de enlace ERCA de segunda generación

— Certificados de enlace MSCA de segunda generación

— Certificados VU de segunda generación expedidos por el mismo país que el propio certificado o certificados de tarjeta de la tarjeta.

Nota: este último requisito implica que una tarjeta deberá poder reconocer la referencia CAR del certificado VU, es decir, el certificado MSCA_VU-EGF. Esta no será la misma referencia que la referencia CAR de su propio certificado, que es el certificado MSCA_Card.

CSM_168 Como se indica en la Figure 5, una vez que la tarjeta ha verificado la autenticidad y validez de un certificado previamente desconocido, puede almacenar este certificado para referencias futuras, de modo que no tenga que volver a verificar la autenticidad del certificado si se vuelve a presentar a la tarjeta. En lugar de almacenar la totalidad del certificado, una tarjeta puede optar por almacenar solamente el contenido del certificado, tal como se especifica en la sección 9.3.2.

10.3. **Autenticación de VU**

CSM_169 Las unidades instaladas en los vehículos utilizarán el protocolo Autenticación de VU ilustrado en la Figure 6 para autenticar la VU ante la tarjeta. La Autenticación de VU permite a la tarjeta de tacógrafo verificar explícitamente que la VU es auténtica. Para ello, la VU utilizará su clave privada para firmar una comprobación generada por la tarjeta.

CSM_170 Junto a la comprobación de la tarjeta, la VU incluirá en la firma la referencia del titular de la tarjeta extraída del certificado de la tarjeta.

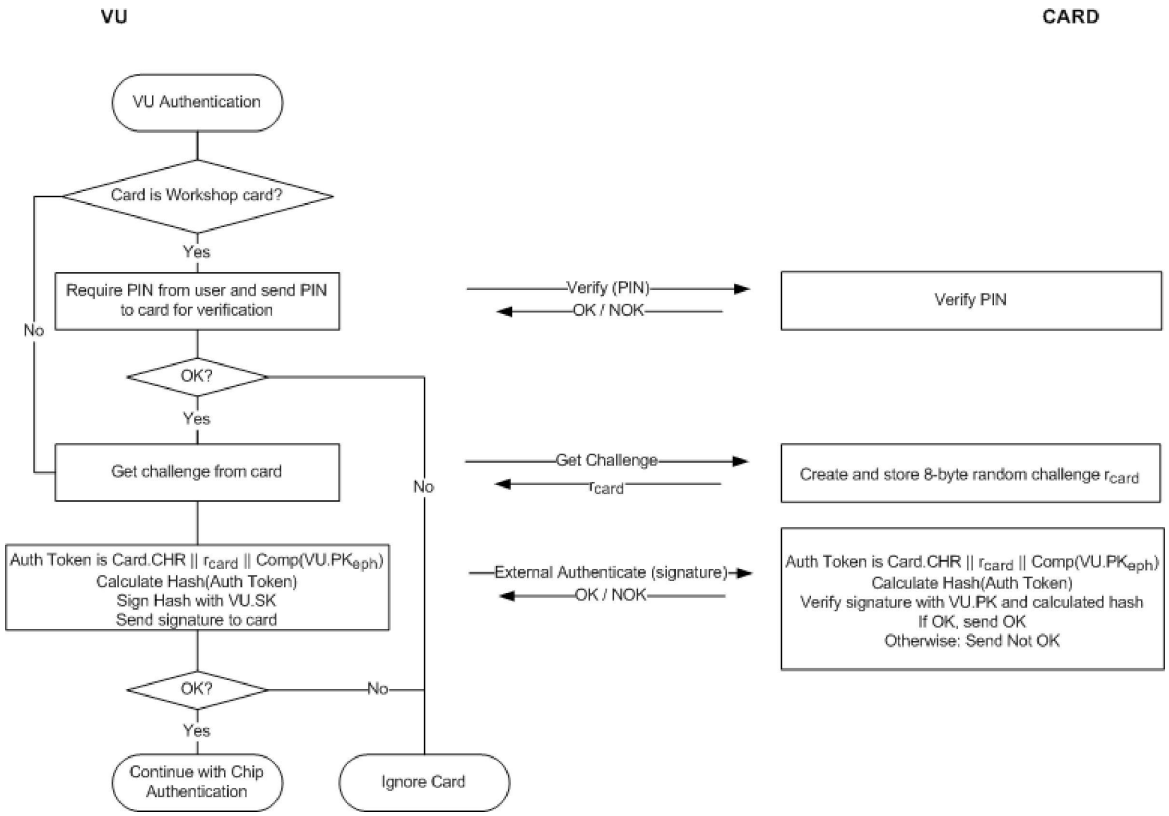
Nota: De esta forma se garantiza que la tarjeta ante la cual se autentica la VU es la misma tarjeta cuya cadena de certificados ha verificado previamente la VU.

CSM_171 La VU incluirá asimismo en la firma el identificador de la clave pública efímera $Comp(VU.PK_{eph})$ que la VU utilizará para establecer la mensajería segura durante el proceso de autenticación del chip especificado en la sección 10.4.

Nota: De esta forma se garantiza que la VU con la que se comunica una tarjeta durante la sesión de mensajería segura es la misma VU que fue autenticada por la tarjeta.

Figura 6

Protocolo de autenticación de VU



CSM_172 Si durante la autenticación de VU la VU envía múltiples comandos GET CHALLENGE, la tarjeta devolverá una nueva comprobación aleatoria de 8 bytes cada vez, pero solamente almacenará la última comprobación.

CSM_173 El algoritmo de firma utilizado por la VU para la autenticación de VU será el algoritmo ECDSA, tal como se especifica en la norma [DSS], utilizando el algoritmo hash relacionado con el tamaño de clave del par de claves VU_MA de la VU, tal como se especifica en CSM_50. El formato de la firma será de texto plano, tal como se especifica en la directriz técnica [TR-03111]. La VU enviará la firma resultante a la tarjeta.

CSM_174 Al recibir la firma de la VU en un comando EXTERNAL AUTHENTICATE, la tarjeta:

— calculará el token de autenticación concatenando Card.CHR, la comprobación de tarjeta r_{card} y el identificador de la clave pública efímera de la VU Comp($VU.PK_{eph}$);

— calculará el algoritmo hash a través del token de autenticación mediante el algoritmo hash relacionado con el tamaño de clave del par de claves VU_MA de la VU, tal como se especifica en CSM_50;

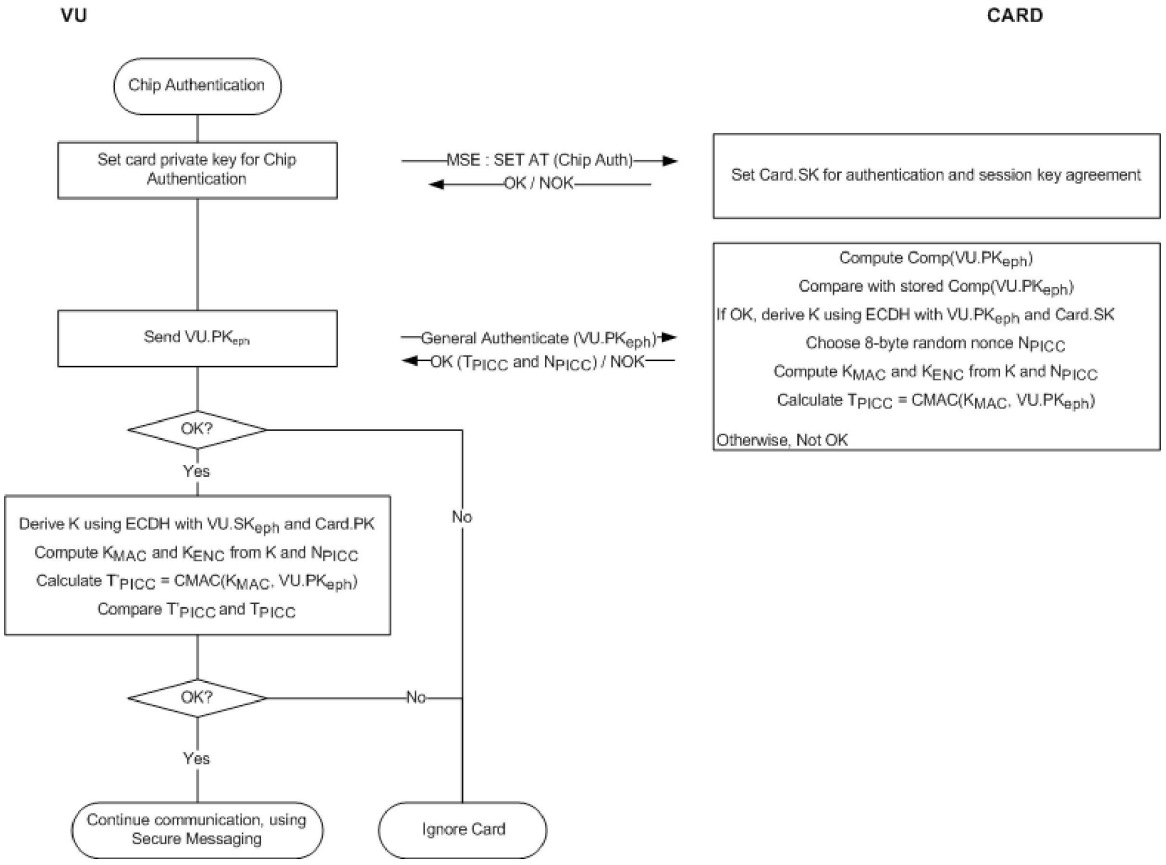
— verificará la firma de la VU mediante el algoritmo ECDSA en combinación con la clave VU.PK y el algoritmo hash calculado.

10.4. Autenticación de chip y acuerdo de claves de sesión

CSM_175 Las unidades instaladas en los vehículos utilizarán el protocolo Autenticación de chip ilustrado en la **Figure 7** para autenticar la tarjeta ante la VU. La Autenticación de chip permite a la unidad instalada en el vehículo verificar explícitamente que la tarjeta es auténtica.

Figure 7

Autenticación de chip y acuerdo de claves de sesión



CSM_176 La VU y la tarjeta efectuarán los siguientes pasos:

1. La unidad instalada en el vehículo inicia el proceso de Autenticación de chip enviando el comando MSE: Set AT que indica 'Autenticación de chip mediante el algoritmo ECDH que resulta en una longitud de clave de sesión AES relacionada con el tamaño de clave del par de claves Card_MA de la tarjeta, tal como se especifica en CSM_50'. La VU determinará el tamaño de clave del par de claves de la tarjeta a partir del certificado de la tarjeta.

2. La VU envía el punto público $VU.PK_{eph}$ de su par de claves efímero a la tarjeta. Como se indica en CSM_164, la VU generó este par de claves efímero antes de la verificación de la cadena de certificados de la VU. La VU envió el identificador de la clave pública efímera $Comp(VU.PK_{eph})$ a la tarjeta, y la tarjeta lo almacenó.

3. La tarjeta computa $Comp(VU.PK_{eph})$ a partir de la clave $VU.PK_{eph}$ y compara el resultado con el valor almacenado de $Comp(VU.PK_{eph})$.

4. Mediante el algoritmo ECDH en combinación con la clave privada estática de la tarjeta y la clave pública efímera de la VU, la tarjeta computa una clave K secreta.

5. La tarjeta selecciona un nonce aleatorio de 8 bytes N_{PICC} mediante el cual deriva dos claves de sesión AES K_{MAC} y K_{ENC} a partir de K. Véase CSM_179.

6. Mediante la clave K_{MAC}, la tarjeta computa un token de autenticación a través del identificador de la clave pública efímera de la VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. La tarjeta envía N_{PICC} y T_{PICC} a la unidad instalada en el vehículo.

7. Mediante el algoritmo ECDH en combinación con la clave privada estática de la tarjeta y la clave pública efímera de la VU, la VU computa la misma clave K secreta que computó la tarjeta en el paso 4.

8. La VU deriva la claves de sesión K_{MAC} y K_{ENC} a partir de K y N_{PICC}; véase CSM_179.

9. La VU verifica el token de autenticación T_{PICC}.

CSM_177 En el paso 3 anterior, la tarjeta computará Comp(VU.PKeph) como la coordenada x del punto publico en VU.PKeph.E

CSM_178 En los pasos 4 y 7 anteriores, la tarjeta y la unidad instalada en el vehículo utilizarán el algoritmo ECKA-EG tal como se define en la directriz técnica [TR-03111].

CSM_179 En los pasos 5 y 8 anteriores, la tarjeta y la unidad instalada en el vehículo utilizarán la función de derivación de clave para las claves de sesión definidas en la directriz técnica [TR-03111], con las siguientes precisiones y cambios:

— El valor del contador será '00 00 00 01' para K_{ENC} y '00 00 00 02' para K_{MAC}.

— Se usará el nonce opcional r igual a N_{PICC}.

— Para derivar claves AES de 128 bits, se deberá utilizar el algoritmo hash SHA-256.

— Para derivar claves AES de 192 bits, se deberá utilizar el algoritmo hash SHA-384.

— Para derivar claves AES de 256 bits, se deberá utilizar el algoritmo hash SHA-512.

La longitud de las claves de sesión (es decir, la longitud a la cual se trunca la función hash) estará relacionada con el tamaño del par de claves Card_MA, tal como se especifica en CSM_50.

CSM_180 En los pasos 6 y 9 anteriores, la tarjeta y la unidad instalada en el vehículo utilizarán el algoritmo en modo CMAC, tal como se especifica en define en la publicación especial del NIST [SP 800-38B]. La longitud de T_{PICC} estará relacionada con la longitud de las claves de sesión AES, tal como se especifica en CSM_50.

10.5. **Mensajería segura**

10.5.1 *Generalidades*

CSM_181 Todos los comandos y respuestas intercambiados entre una unidad instalada en el vehículo y una tarjeta de tacógrafo tras la autenticación correcta del chip y hasta el final de la sesión estarán protegidos por mensajería segura.

CSM_182 Salvo durante la lectura en un archivo con la condición de acceso SM-R-ENC-MAC-G2 (véase el apéndice 2, sección 4), la mensajería segura se utilizará en modo solo autenticación. En este modo, una suma de comprobación criptográfica, también llamada código de autenticación de mensajes (MAC), se añade a todos los comandos y respuestas para garantizar la autenticidad e integridad de los mensajes.

CSM_183 Al leer los datos de un archivo con la condición de acceso SM-R-ENC-MAC-G2, la mensajería segura se utilizará en el modo cifrar y después autenticar, es decir, primero se cifran los datos de respuesta para asegurar la confidencialidad del mensaje, y después se calcula un MAC con los datos cifrados formateados para asegurar la autenticidad e integridad.

CSM_184 La mensajería segura utilizará la norma AES tal como se define en [AES] con las claves de sesión K_{MAC} y K_{ENC} acordadas durante la autenticación del chip.

CSM_185 Se utilizará un entero no firmado como contador de envío de secuencia (SSC) para impedir los ataques por repetición. El tamaño del SSC será igual al tamaño de bloque AES. es decir, 128 bits. El SSC tendrá el formato MSB primero. El contador de envío de secuencia se inicializará a cero (es decir, '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00') cuando se inicie la mensajería segura. El SSC se incrementará cada vez antes de generar un comando o respuesta APDU, es decir, puesto que el valor de inicio del SSC en una sesión SM es 0, en el primer comando el valor del SSC será 1. El valor de SCC para la primera respuesta será 2.

CSM_186 Para el cifrado de mensajes se utilizará la clave K_{ENC} con AES en el modo de operación de encadenamiento de bloques de cifrado (CBC), tal como se define en la norma [ISO 10116], con un parámetro interpolar $m = 1$ y un vector de inicialización $SV = E(K_{ENC}, SSC)$, es decir, el valor actual del contador de envío de secuencia cifrado con la clave K_{ENC}.

CSM_187 Para la autenticación de mensajes, se utilizará la clave K_{MAC} con AES en el modo CMAC, tal como se especifica en la publicación especial [SP 800-38B]. La longitud del MAC estará relacionada con la longitud de las claves de sesión AES, tal como se especifica en CSM_50. El contador de envío de secuencia se incluirá en el MAC copiándolo al principio antes del datagrama que se deba autenticar.

10.5.2 *Estructura de mensaje segura*

CSM_188 La mensajería segura utilizará solamente los objetos de datos de mensajería segura (véase la norma [ISO 7816-4]) enumerados en la Table 5. En cualquier mensaje, estos objetos de datos se utilizarán en el orden especificado en esta tabla.

Tabla 5

Objetos de datos de mensajería segura

Nombre de objeto de datos	Etiqueta	Presencia obligatoria (M), condicional (C) o prohibida (F) en	
		Comandos	Respuestas
Valor plano no codificado en BERL-TLV	'81'	C	C
Valor plano codificado en BERL-TLV, pero excluidos los DO de SM	'B3'	C	C
Indicador de contenido de relleno seguido de criptograma, valor plano no codificado en BER-TLV	'87'	C	C
Le protegida	'97'	C	F
Estado de procesamiento	'99'	F	M
Suma de control criptográfica	'8E'	M	M

Nota: Tal como se especifica en el apéndice 2, las tarjetas de tacógrafo pueden soportar el comando READ BINARY y UPDATE BINARY con un byte INS impar ('B1' resp. 'D7'). Estas variantes de comando son necesarias para leer y actualizar ficheros de 32 768 bytes o más. En el caso de que se utilice una variante, en lugar de un objeto con la etiqueta '81' se utilizará un objeto de datos con la etiqueta 'B3'. Véase el apéndice 2 para más información.

CSM_189 Todos los objetos de datos de SM (mensajería segura) se codificarán en DER TLV, tal como se especifica en la norma [ISO 8825-1]. Esta codificación resulta en una estructura etiqueta-longitud-valor (TLV) como la siguiente:

Etiqueta: La etiqueta está codificada en uno o dos octetos e indica el contenido.

Longitud: La longitud está codificada como un número entero no firmado en uno, dos, o tres octetos, que resultan en una longitud máxima de 65 535 octetos. Se utilizará el número de octetos mínimo.

Valor: El valor está codificado en cero o más octetos.

CSM_190 Las unidades de datos de protocolo de aplicación (APDU) protegidas mediante mensajería segura se crearán de la siguiente manera:

— La cabecera de comando se incluirá en el cálculo del MAC, por consiguiente, para el byte de clase CLA se utilizará el valor '0C'.

— Como se especifica en el apéndice 2, todos los bytes INS serán pares, con la posible excepción de bytes INS impares para los comandos READ BINARY y UPDATE BINARY.

— El valor real de Lc se modificará a Lc' tras la aplicación de la mensajería segura.

— El campo Datos estará compuesto de objetos de datos SM.

— En el comando protegido APDU, el nuevo byte Le se configurará a '00'. En caso necesario, el objeto de datos '97' se incluirá en el campo Datos a fin de comunicar el valor original de Le.

CSM_191 Los objetos de datos que deban cifrarse se rellenarán de acuerdo con la norma [ISO 7816-4] mediante el indicador de contenido de relleno '01'. Para el cálculo del MAC, cada objeto de datos de la APDU se rellenará también separadamente conforme a la norma [ISO 7816-4].

Nota: El relleno para la mensajería segura siempre es efectuado por la capa de mensajería segura, no por los algoritmos CMAC o CBC.

Resumen y ejemplos

Un comando APDU con mensajería segura aplicada tendrá la siguiente estructura, dependiendo del caso del comando no securizado correspondiente (DO significa objeto de datos):

Caso 1:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Caso 2:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Caso 3 (byte INS par):	CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le
Caso 3 (byte INS impar):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le
Caso 4 (byte INS par):	CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le
Caso 4 (byte INS impar):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

donde Le = '00' o '00 00', dependiendo de si se usan campos de corta longitud o de longitud extendida; véase la norma [ISO 7816-4].

Una respuesta APDU con mensajería segura aplicada tendrá la siguiente estructura, dependiendo del caso del comando no securizado correspondiente:

Caso 1 o 3:	DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS par) con cifrado:	DO '81' || DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS par) sin cifrado:	DO '87' || DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS impar) sin cifrado:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

Nota: El caso 2 o 4 (byte INS impar) con cifrado no se usa nunca en la comunicación entre una VU y una tarjeta.

A continuación figuran tres ejemplos de transformaciones APDU para comandos con código INS par. La Figure 8 muestra un comando APDU de caso 4 autenticado, la Figure 9 muestra una respuesta APDU de caso 2/caso 4 autenticada, y la Figure 10 muestra una respuesta APDU de caso 2/caso 4 cifrada y autenticada.

Figura 8

Transformación de un comando APDU de caso 4 autenticado

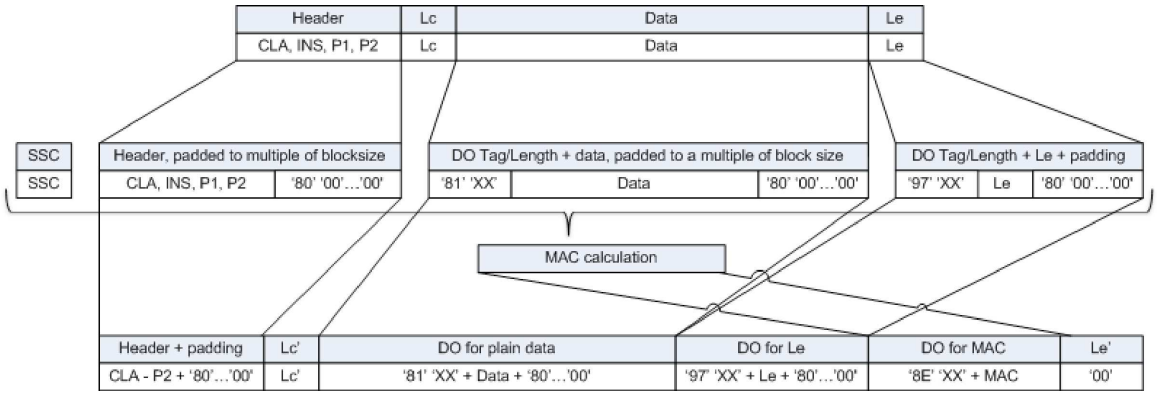


Figura 9

Transformación de una respuesta APDU de caso 1/caso 3 autenticada

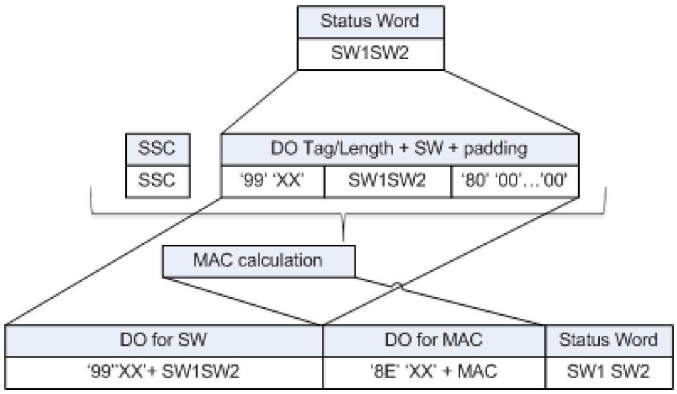
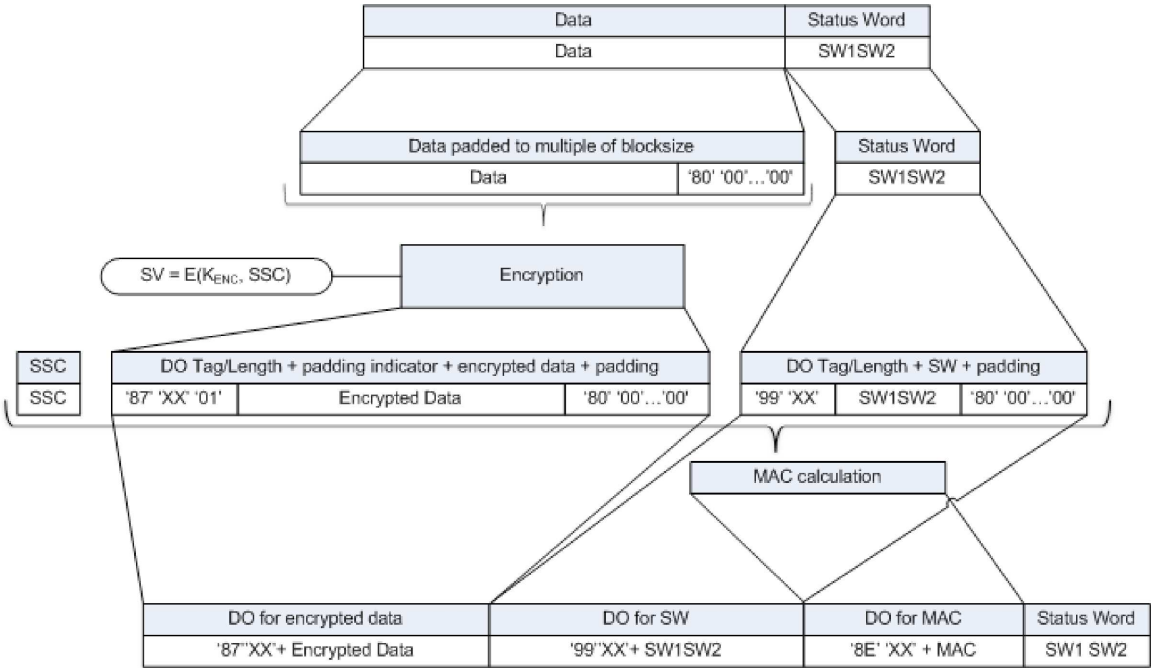


Figura 10

Transformación de una respuesta APDU de caso 2/caso 4 cifrada y autenticada



10.5.3 *Aborto de sesión de mensajería segura*

CSM_192 Una unidad instalada en el vehículo abortará una sesión de mensajería segura en curso solamente si si se da una de las condiciones siguientes:

— recibe una respuesta APDU plana;

— detecta un error de mensajería segura en una respuesta APDU:

— falta un objeto de datos de mensajería segura esperado, el orden de los objetos de datos es incorrecto, o hay incluido un objeto de datos desconocido;

— un objeto de datos de mensajería segura es incorrecto, por ejemplo, el valor MAC es incorrecto, la estructura TLC es incorrecta, o el indicador de relleno de la etiqueta '87' no es igual a '01';

— la tarjeta envía un byte de estado que indica que ha detectado un error SM (véase CSM_194);

— se ha alcanzado el límite de número de comandos y respuestas asociadas en la sesión actual. Este límite lo definirá para cada VU concreta su fabricante, teniendo en cuenta los requisitos de seguridad del soporte físico utilizado, con un valor máximo de 240 comandos y respuestas asociadas de SM por sesión.

CSM_193 Una tarjeta de tacógrafo abortará una sesión de mensajería segura en curso solamente si se da una de las condiciones siguientes:

— recibe un comando APDU plano;

— detecta un error de mensajería segura en un comando APDU:

— falta un objeto de datos de mensajería segura esperado, el orden de los objetos de datos es incorrecto, o hay incluido un objeto de datos desconocido;

— un objeto de datos de mensajería segura es incorrecto, por ejemplo, el valor MAC es incorrecto o la estructura TLC es incorrecta;

— no recibe alimentación eléctrica o ha sido restaurada;

— la VU selecciona una aplicación de la tarjeta;

— la VU inicia el proceso de autenticación de la VU;

— se ha alcanzado el límite de número de comandos y respuestas asociadas en la sesión actual. Este límite lo definirá para cada tarjeta concreta su fabricante, teniendo en cuenta los requisitos de seguridad del soporte físico utilizado, con un valor máximo de 240 comandos y respuestas asociadas de SM por sesión.

CSM_194 En relación con la gestión de errores SM por la tarjeta de tacógrafo:

— Si en un comando APDU faltan objetos de datos de mensajería segura esperados, el orden de los objetos de datos es incorrecto, o hay incluidos objetos de datos incorrectos o desconocidos, la tarjeta de tacógrafo responderá con los bytes de estado '69 87'.

— Si un objeto de datos de mensajería segura en un comando APDU es incorrecto, la tarjeta de tacógrafo responderá con los bytes de estado '69 88'.

En tal caso, los bytes de estado se devolverán sin usar la mensajería segura.

CSM_195 Si una sesión de mensajería segura entre una VU y una tarjeta de tacógrafo se aborta, la VU y la tarjeta de tacógrafo:

— destruirá de forma segura las claves de sesión almacenadas;

— establecerá inmediatamente una nueva sesión de mensajería segura, como se describe en las secciones 10.2 — 10.5.

CSM_196 Si, por cualquier razón, la VU decide reiniciar la autenticación mutua frente a una tarjeta insertada, el proceso se reiniciará con la verificación de la cadena de certificados de la tarjeta, tal como se describe en la sección 10.2, y continuará en la forma descrita en las secciones 10.2 — 10.5.

11. ACOPLAMIENTO, AUTENTICACIÓN MUTUA Y MENSAJERÍA SEGURA ENTRE LA VU Y EL DISPOSITIVO GNSS EXTERNO

11.1. **Generalidades**

CSM_197 El dispositivo GNSS utilizado por una VU para determinar su posición puede ser interna (es decir, montada dentro de la caja de la VU y no separable), o puede ser un módulo externo. En el primer caso, no hay necesidad de normalizar la comunicación interna entre el dispositivo GNSS y la VU, y los requisitos del presente capítulo no son de aplicación. En el último caso, la comunicación entre la VU y el dispositivo GNSS externo estará normalizada y protegida tal como se describe en este capítulo.

CSM_198 La comunicación segura entre una unidad instalada en el vehículo y un dispositivo GNSS externo tendrá lugar de la misma forma que una comunicación segura entre una unidad instalada en el vehículo y una tarjeta de tacógrafo, donde el dispositivo GNSS externo (EGF) tiene la función de tarjeta. Las EGF cumplirá todos los requisitos mencionados en el capítulo 10 para las tarjetas de tacógrafo teniendo en cuenta las desviaciones, clarificaciones y añadidos mencionados en el presente capítulo. En particular, la verificación mutua de la cadena de certificados, la autenticación de la VU y la autenticación del chip se efectuará tal como se describe en las secciones 11.3 y 11.4.

CSM_199 La comunicación entre una unidad instalada en el vehículo y una EGF difiere de la comunicación entre una unidad instalada en el vehículo y una tarjeta en que una unidad instalada en el vehículo y una EGF deben acoplarse una vez en un taller antes de que la VU y la EGF puedan intercambiar datos basados en el GNSS durante el funcionamiento normal. El proceso de acoplamiento se describe en la sección 11.2.

CSM_200 Para la comunicación entre una unidad instalada en el vehículo y una EGF, se usarán los comandos y respuestas APDU basados en las normas [ISO 7816-4] e [ISO 7816-8]. La estructura exacta de estas APDU está definida en el apéndice 2 del presente anexo.

11.2. **Acoplamiento entre la VU y el dispositivo GNSS externo**

CSM_201 Una unidad instalada en el vehículo y una EGF de un vehículo se acoplarán en un taller. En funcionamiento normal, solamente se podrán comunicar una unidad instalada en el vehículo y una EGF acopladas.

CSM_202 El acoplamiento de una unidad instalada en el vehículo y una EGF solamente será posible si la unidad instalada en el vehículo está en modo calibración. El acoplamiento será iniciado por la unidad instalada en el vehículo.

CSM_203 Un taller puede reacoplar una unidad instalada en el vehículo a otra EGF o a la misma EGF en cualquier momento. Durante el reacoplamiento, la VU destruirá de forma segura el certificado EGF_MA existente en su memoria y almacenará el certificado EGF_MA de la EGF a la que esté siendo acoplada.

CSM_204 Un taller puede reacoplar un dispositivo GNSS externo a otra VU o a la misma VU en cualquier momento. Durante el reacoplamiento, la EGF destruirá de forma segura el certificado VU_MA existente en su memoria y almacenará el certificado VU_MA de la VU a la que esté siendo acoplada.

11.3. **Verificación mutua de la cadena de certificados**

11.3.1 *Generalidades*

CSM_205 La verificación mutua de la cadena de certificados entra una VU y una EGF se efectuará solamente durante el acoplamiento de la VU y la EGF por un taller. Durante el funcionamiento normal de una VU y una EGF acopladas, no se verificará ningún certificado. En lugar de eso, la VU y la EGF confiarán en los certificados que hayan almacenado durante el acoplamiento, una vez comprobada la validez temporal de los mismos. La VU y la EGF no confiarán en ningún otro certificado para proteger la comunicación entre la VU y la EGF durante el funcionamiento normal.

11.3.2 *Durante el acoplamiento entre la VU y la EGF*

CSM_206 Durante el acoplamiento a una EGF, la unidad instalada en el vehículo utilizará el protocolo ilustrado en la Figure 4 (sección 10.2.1) para verificar la cadena de certificados del dispositivo GNSS externo.

Notas de la Figure 4 en este contexto.

— El control de la comunicación está fuera del ámbito del presente apéndice. No obstante, una EGF no es una tarjeta inteligente y, por consiguiente, la VU probablemente no mandará un comando Restaurar (Reset) para iniciar la comunicación y no recibirá una respuesta ATR.

— Los certificados de tarjeta y las claves públicas mencionadas en la figura se interpretarán como los certificados de la EGF y las claves públicas para autenticación mutua. La sección 9.1.6 los denota EGF_MA.

— Los certificados de tarjeta Card.CA y las claves públicas mencionadas en la figura se interpretarán como los certificados de la MSCA y las claves públicas para firmar certificados EGF. La sección 9.1.3 los denota MSCA_VU-EGF.

— El certificado Card.CA.EUR mencionado en la figura se interpretará como el certificado raíz europeo indicado en la referencia CAR del certificado MSCA_VU-EGF.

— El certificado Card.Link mencionado en la figura se interpretará como el certificado de enlace de la EGF, si está presente. Tal como se especifica en la sección 9.1.2, este es el certificado de enlace para un nuevo par de claves raíz europeo creado por la ERCA y firmado por la clave privada europea anterior.

— El certificado Card.Link.EUR es el certificado raíz europeo indicado en la referencia CAR del certificado Card.Link.

— En lugar del `cardExtendedSerialNumber`, la VU leerá el `sensorGNSSserialNumber` del archivo EF ICC.

— En lugar de seleccionar el AID del tacógrafo, la VU seleccionará el AID de la EGF.

— 'Ignore Card' se interpretará como 'Ignore EGF'.

CSM_207 Una vez verificado el certificado EGF_MA, la unidad instalada en el vehículo almacenará el certificado para utilizarlo durante el funcionamiento normal. Véase la sección 11.3.3.

CSM_208 Durante el acoplamiento a una VU, una unidad GNSS externa utilizará el protocolo ilustrado en la Figure 5 (sección 10.2.2) para verificar la cadena de certificados de la VU.

Notas de la Figure 5 en este contexto.

— La VU generará un nuevo par de claves efímero utilizando los parámetros de dominio del certificado EGF.

— Los certificados de VU y las claves públicas mencionados en la figura son los empleados para la autenticación mutua. La sección 9.1.4 los denota VU_MA.

— Los certificados VU.CA y las claves públicas mencionados en la figura son los empleados para firmar los certificados de VU y de dispositivo GNSS externo. La sección 9.1.3 los denota MSCA_VU-EGF.

— El certificado VU.CA.EUR mencionado en la figura es el certificado raíz europeo indicado en la referencia CAR del certificado VU.CA.

— El certificado VU.Link mencionado en la figura es el certificado de enlace de la VU, si está presente. Tal como se especifica en la sección 9.1.2, este es el certificado de enlace para un nuevo par de claves raíz europeo creado por la ERCA y firmado por la clave privada europea anterior.

— El certificado VU.Link.EUR es el certificado raíz europeo indicado en la referencia CAR del certificado VU.Link.

CSM_209 En caso de desviación del requisito CSM_167, una EGF utilizará la hora del GNSS para verificar la validez temporal de cualquier certificado presentado.

CSM_210 Una vez verificado el certificado VU_MA, la unidad GNSS externa almacenará el certificado para utilizarlo durante el funcionamiento normal. Véase la sección 11.3.3.

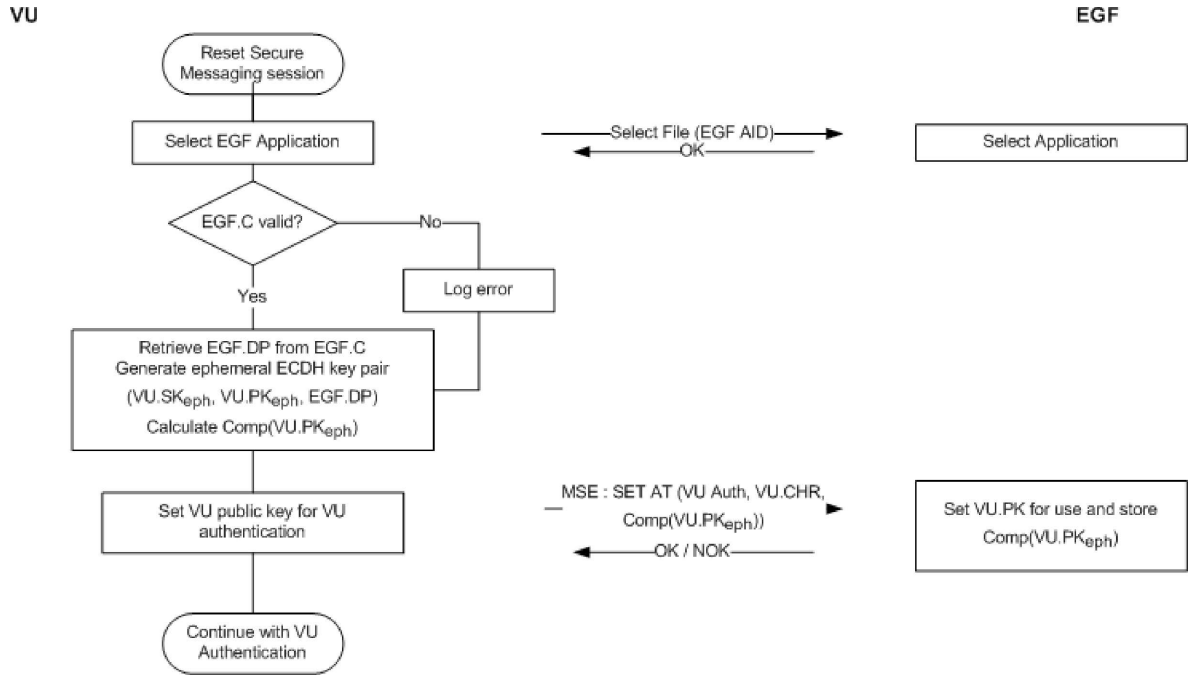
11.3.3 *Durante el funcionamiento normal*

CSM_211 Durante el funcionamiento normal, una unidad instalada en el vehículo y una EGF utilizarán el protocolo ilustrado en la Figure 11 para verificar la validez temporal de los certificados EGF_MA y VU_MA almacenados y para configurar la clave pública VU_MA para la posterior autenticación de la VU. Durante el funcionamiento normal no se efectuará ninguna nueva verificación mutua de las cadenas de certificados.

Obsérvese que la Figure 11 consiste en esencia de los primeros paso mostrados en la Figure 4 y en la Figure 5. Asimismo, obsérvese que puesto que una EGF no es una tarjeta inteligente, la VU probablemente no mandará un comando Restaurar (Reset) para iniciar la comunicación y no recibirá una respuesta ATR. En cualquier caso, esto está fuera del ámbito del presente apéndice.

Figura 11

Verificación mutua de la validez temporal del certificado durante el funcionamiento normal de la VU — EGF.



CSM_212 Tal como muestra la Figure 11, la unidad instalada en el vehículo registrará un error si el certificado EGF_MA ha caducado. No obstante, la autenticación mutua, el acuerdo de claves y la comunicación subsiguiente a través de la mensajería segura procederán normalmente.

11.4. Autenticación de la VU, autenticación del chip y acuerdo de claves de sesión

CSM_213 La autenticación de la VU, la autenticación del chip y el acuerdo de claves de sesión entre una VU y una EGF se efectuarán durante el acoplamiento y siempre que se restablezca una sesión de mensajería segura durante el funcionamiento normal. La VU y la EGF efectuarán los procesos descritos en las secciones 10.3 y 10.4. Todos los requisitos de estas secciones serán de aplicación.

11.5. Mensajería segura

CSM_214 Todos los comandos y respuestas intercambiados entre una unidad instalada en el vehículo y un dispositivo GNSS externo tras la autenticación correcta del chip y hasta el final de la sesión estarán protegidos por mensajería segura en modo solo autenticación. Todos los requisitos de la sección 10.5 serán de aplicación.

CSM_215 Si una sesión de mensajería segura entra una VU y una EGF se aborta, la VU establecerá inmediatamente una nueva sesión de mensajería segura, tal como se describe en las secciones 11.3.3 y 11.4.

12. EMPAREJAMIENTO Y COMUNICACIÓN ENTRE UNA VU Y UN SENSOR DE MOVIMIENTO

12.1. **Generalidades**

CSM_216 Una unidad instalada en el vehículo y un sensor de movimiento se comunicarán mediante el protocolo de interfaz especificado en la norma [ISO 16844-3] durante el emparejamiento y el funcionamiento normal, con los cambios descritos en el presente capítulo y en la sección 9.2.1.

Nota: se supone que los lectores del presente capítulo están familiarizados con el contenido de la norma [ISO 16844-3].

12.2. **Emparejamiento de la VU con el sensor de movimiento mediante claves de diferentes generaciones**

Como se explica en la sección 9.2.1, la clave maestra del sensor de movimiento y todas las claves asociadas son sustituidas regularmente. Esta circunstancia da lugar a la presencia de hasta tres claves AES K_{M-WC} (de generaciones de claves consecutivas) relacionadas con los sensores de movimiento en las tarjetas de taller. Análogamente, en los sensores de movimiento puede haber hasta tres cifrados de datos diferentes basados en algoritmos AES resultantes de generaciones consecutivas de la clave maestra K_M del sensor de movimiento. Una unidad instalada en el vehículo contiene solamente una clave K_{M-VU} relacionada con el sensor de movimiento.

CSM_217 Una VU de segunda generación y un sensor de movimiento de segunda generación se emparejarán de la siguiente manera (compárese la tabla 6 de la norma [ISO 16844-3]):

1. Una tarjeta de taller de segunda generación se inserta en la VU, y la VU se conecta al sensor de movimiento.

2. La VU lee todas las claves K_{M-WC} disponibles en la tarjeta de taller, inspecciona sus números de versión de clave y selecciona la que tiene el número correspondiente al de la versión de la clave K_{M-VU} de la VU. Si la clave K_{M-WC} correspondiente no está presente en la tarjeta de taller, la VU aborta el proceso de emparejamiento y muestra un mensaje de error apropiado al titular de la tarjeta de taller.

3. La VU calcula la clave maestra K_M del sensor de movimiento a partir de K_{M-VU} y K_{M-WC} y la clave de identificación K_{ID} a partir de K_M, tal como se especifica en la sección 9.2.1.

4. La VU envía la instrucción para iniciar el proceso de emparejamiento al sensor de movimiento, tal como se describe en la norma [ISO 16844-3], y cifra el número de serie que recibe del sensor de movimiento con la clave de identificación K_{ID}. La VU envía el número de serie cifrado al sensor de movimiento.

5. El sensor de movimiento compara el número de serie cifrado consecutivamente con cada cifrado del número de serie que contiene internamente. Si encuentra una correspondencia, se autentica la VU. El sensor de movimiento anota la clave de generación K_{ID} utilizada por la VU y devuelve la versión cifrada correspondiente de su clave de emparejamiento; es decir, el cifrado creado mediante la misma generación de K_M.

6. La VU descifra la clave de emparejamiento mediante la clave K_M, genera una clave de sesión K_S, la cifra con la clave de emparejamiento y envía el resultado al sensor de movimiento. El sensor de movimiento descifra la clave K_S.

7. La VU ensambla la información de emparejamiento tal como se define en la norma [ISO 16844-3], cifra la información con la clave de emparejamiento, y envía el resultado al sensor de movimiento. El sensor de movimiento descifra la información de emparejamiento.

8. El sensor de movimiento cifra la información de emparejamiento recibida con la clave K_S recibida y la envía a la VU. La VU verifica que la información de emparejamiento es la misma información que la que la VU envió al sensor de movimiento en el paso anterior. Si lo es, esto prueba que el sensor de movimiento utilizó la misma clave K_S que la VU y, por consiguiente, en el paso 5 envió su clave de emparejamiento cifrada con la clave K_M de la generación correcta. Por tanto, el sensor de movimiento es autenticado.

Obsérvese que los pasos 2 y 5 son diferentes del proceso normal definido en la norma ISO 16844-3]; los demás pasos son normales.

Ejemplo: Supóngase que un emparejamiento se efectúa durante el primer año de validez del certificado ERCA (3); véase la Figure 2 en la sección 9.2.1.2. Además

— Supóngase que el sensor de movimiento fue expedido durante el último año de validez del certificado ERCA (1). Por consiguiente contendrá las siguientes claves y datos:

  — $N_s[1]$: su número de serie cifrado con la generación 1 de la clave K_{ID}

  — $N_s[2]$: su número de serie cifrado con la generación 2 de la clave K_{ID}

  — $N_s[3]$: su número de serie cifrado con la generación 3 de la clave K_{ID}

  — $K_P[1]$: su clave de emparejamiento de generación 1 ([1]), cifrada con la generación 1 de la clave K_M

  — $K_p[2]$: su clave de emparejamiento de generación 2, cifrada con la generación 2 de la clave K_M

  — $K_P[3]$: su clave de emparejamiento de generación 3, cifrada con la generación 3 de la clave K_M

— Supóngase que la tarjeta de taller fue expedida durante el último año de validez del certificado ERCA (3). Por tanto contendrá la generación 2 y la generación 3 de la clave $K_{M\text{-}WC}$.

— Supóngase que la VU es una VU de generación 2 que contiene la generación 2 de la clave $K_{M\text{-}VU}$.

En este caso, en los pasos 2 a 5 ocurrirá lo siguiente:

— Paso 2: La VU lee la generación 2 y la generación 3 de la clave $K_{M\text{-}WC}$ en la tarjeta de taller e inspecciona sus números de versión.

— Paso 3: La VU combina la clave $K_{M\text{-}WC}$ de generación 2 con su clave $K_{M\text{-}VU}$ para computar las claves $K_{M\ y}$ K_{ID}.

— Paso 4: La VU cifra el número de serie que recibe del sensor de movimiento con la clave K_{ID}.

— Paso 5: El sensor de movimiento compara los datos recibidos con $N_s[1]$ y no encuentra una correspondencia. Seguidamente, compara los datos con $N_s[2]$ y encuentra una correspondencia. Concluye que la VU es de generación 2, y por tanto devuelve la clave $K_p[2]$.

12.3. Emparejamiento y comunicación entre una VU y un sensor de movimiento mediante el algoritmo AES

CSM_218 Tal como se especifica en la Table 3 de la sección 9.2.1, todas las claves involucradas en el emparejamiento de una unidad instalada en el vehículo (de segunda generación) y un sensor de movimiento y en la comunicación subsiguiente serán claves AES, en lugar de las claves TDES de doble longitud especificadas en la norma [ISO 16844-3]. Estas claves AES pueden tener una longitud de 128, 192 o 256 bits. Puesto que el AES tiene un tamaño de bloque de 16 bytes, la longitud del mensaje cifrado deberá ser un múltiplo de 16 bytes, en comparación con los 8 bytes para el TDES. Además. algunos de estos mensajes se utilizarán para transportar claves AES cuya longitud puede ser de 128, 192 o 256 bits. Por consiguiente, el número de bytes de datos por instrucción de la tabla 5 de la norma [ISO 16844-3] se modificará tal como ilustra la Table 6:

Tabla 6

Número de bytes de datos de texto plano y cifrados por instrucción definido en la norma in [ISO 16844-3]

Instrucción	Solicitud/ respuesta	Descripción de los datos	# de bytes de texto plano según la norma [ISO 16844-3]	# de bytes de datos de texto plano mediante claves AES	# de bytes de datos cifrados mediante claves AES de longitud en bits de		
					128	192	256
10	solicitud	Datos de autenticación + número de archivo	8	8	16	16	16

([1]) Obsérvese que las claves de emparejamiento de generación 1, generación 2 y generación 3 pueden de hecho ser la misma clave, o bien pueden ser tres claves distintas de tres longitudes diferentes, tal como se explica en CSM_117.

Instrucción	Solicitud/ respuesta	Descripción de los datos	# de bytes de texto plano según la norma [ISO 16844-3]	# de bytes de datos de texto plano mediante claves AES	# de bytes de datos cifrados mediante claves AES de longitud en bits de		
					128	192	256
11	respuesta	Datos de autenticación + contenido de archivo	16 o 32, según el archivo	16 o 32, según el archivo	16 / 32	16 / 32	16 / 32
41	solicitud	Nº de serie del sensor	8	8	16	16	16
41	respuesta	Clave de emparejamiento	16	16 / 24 / 32	16	32	32
42	solicitud	Clave de sesión	16	16 / 24 / 32	16	32	32
43	solicitud	Información de emparejamiento	24	24	32	32	32
50	respuesta	Información de emparejamiento	24	24	32	32	32
70	solicitud	Datos de autenticación	8	8	16	16	16
80	respuesta	Valor de contador del sensor + datos de autenticación	8	8	16	16	16

CSM_219 La información de emparejamiento enviada en las instrucciones 43 (solicitud de la VU) y 50 (respuesta del sensor de movimiento) se ensamblará tal como se especifica en la sección 7.6.10 de la norma [ISO 16844-3], salvo que se usará el algoritmo AES en lugar del algoritmo TDES en el esquema criptográfico basado en el emparejamiento de datos, lo que resulta en dos cifrados AES, y se adoptará el relleno especificado en CSM_220 a fin de adecuarla al tamaño de bloque del AES. La clave K'_P usada para este cifrado se generará de la siguiente manera:

— En el caso de que la clave de emparejamiento K_P sea de 16 bytes de longitud: $K'_P = K_P$ XOR ($N_s||N_s$)

— En el caso de que la clave de emparejamiento K_P sea de 24 bytes de longitud: $K'_P = K_P$ XOR ($N_s||N_s||N_s$)

— En el caso de que la clave de emparejamiento K_P sea de 32 bytes de longitud: $K'_P = K_P$ XOR ($N_s||N_s||N_s||N_s$)

donde N_s es el número de serie de 8 bytes del sensor de movimiento.

CSM_220 En el caso de que la longitud de datos de texto plano (con claves AES) no sea un múltiplo de 16 bytes, se usará el método de relleno 2 definido en la norma [ISO 9797-1].

Nota: en la norma [ISO 16844-3], el número de bytes de datos de texto plano es siempre un múltiplo de 8, de tal modo que no se necesita relleno si se usa el algoritmo TDES. Esta parte del presente apéndice no modifica la definición de datos y mensajes en la norma [ISO 16844-3], y por tanto exige la aplicación de relleno.

CSM_221 Para la instrucción 11 y en el caso de que deba cifrarse más de un bloque de datos, se usará el modo de operación de encadenamiento de bloques de cifrado tal como se define en la norma [ISO 10116], con un parámetro interpolar $m = 1$. El vector de inicialización que se deberá utilizar será el siguiente:

— Para la instrucción 11: El bloque de autenticación de 8 bytes especificado en la sección 7.6.3.3 de la norma [ISO 16844-3], rellenado mediante el método de relleno 2 definido en la norma [ISO 9797-1]; véanse asimismo las secciones 7.6.5 y 7.6.6 de la norma [ISO 16844-3].

— Para todas las demás instrucciones en las que se transfieran más de 16 bytes, tal como se especifica en la Table 6: '00'{16}, es decir, dieciséis bytes de valor binario 0.

Nota: Tal como muestran las secciones 7.6.5 y 7.6.6 de la norma [ISO 16844-3]., cuando el sensor de movimiento cifra archivos de datos para su inclusión en la instrucción 11, el bloque de autenticación

— se usa como vector de inicialización para el cifrado en modo de encadenamiento de bloques de cifrado de los archivos de datos, y

— se cifra e incluye como el primer bloque en los datos enviados a la VU.

12.4. **Emparejamiento del sensor de movimiento para equipos de diferentes generaciones**

CSM_222 Como se explica en la sección 9.2.1, un sensor de movimiento de segunda generación puede contener el cifrado basado en el algoritmo TDES de los datos de emparejamiento (tal como se define en la parte A del presente apéndice), lo que permite emparejar el sensor de movimiento con una VU de primera generación. Si es el caso, una VU de primera generación y un sensor de movimiento de segunda generación se emparejarán en la forma descrita en la parte A del presente apéndice y en la norma [ISO 16844-3]. Para el proceso de emparejamiento puede usarse una tarjeta de taller de primera generación o de segunda generación.

Notas:

— No es posible emparejar una VU de segunda generación con un sensor de movimiento de primera generación.

— No es posible usar una tarjeta de taller de primera generación para emparejar una VU de segunda generación con un sensor de movimiento.

13. SEGURIDAD PARA LA COMUNICACIÓN REMOTA MEDIANTE DSRC

13.1. **Generalidades**

Tal como se especifica en el apéndice 14, una VU genera regularmente datos de monitorización remota de tacógrafos (RTM) y los envía a la instalación (interna o externa) de comunicación remota (RCF). La instalación de comunicación remota es responsable de enviar estos datos por la interfaz descrita en el apéndice 14 al interrogador remoto. El apéndice 1 especifica que los datos RTM son la concatenación de:

Carga útil cifrada del tacógrafo el cifrado de la carga útil de texto plano del tacógrafo

Datos de seguridad DSRC descritos a continuación

El formato de los datos de carga útil de texto plano del tacógrafo se especifica en el apéndice 1 y se describe en mayor profundidad en el apéndice 14. Esta sección describe la estructura de los datos de seguridad DSRC; la especificación formal está en el apéndice 1.

CSM_223 Los datos `tachographPayload` de texto plano comunicados por una VU a una instalación de comunicación remota (si la ICF es externa) o de la VU a un interrogador remoto a través de la interfaz DSRC (si la RCF es interna) se protegerán en modo cifrar y después autenticar, es decir, primero se cifran los datos de carga útil del tacógrafro para asegurar la confidencialidad del mensaje, y después se calcula un código MAC para asegurar la autenticidad e integridad de los datos.

CSM_224 Los datos de seguridad DSRC estarán compuestos de la concatenación de los siguientes elementos de datos en el orden siguiente: véase también la Figure 12:

Fecha y hora actual	la fecha y hora actual de la VU (tipo de dato `TimeReal`)
Contador	un contador de 3 bytes, véase CSM_225

Nº de serie de la VU	el número de serie de la VU (tipo de dato `VuSerialNumber`)
Nº de versión de la clave maestra DSRC	el número de versión de 1 byte de la clave maestra DSRC de la que se derivaron las claves DSRC específicas de la VU; véase la sección 9.2.2.
MAC	el MAC calculado a través de todos los bytes anteriores en los datos RTM.

CSM_225 El contador de 3 bytes en los datos de seguridad DSRC estará en el formato MSB-primero. La primera vez que una VU calcule un conjunto de datos RTM tras su puesta en funcionamiento, configurará el valor del contador en 0. Antes de calcular el siguiente conjunto de datos RTM, la VU incrementará cada vez el valor de los datos del contador en 1.

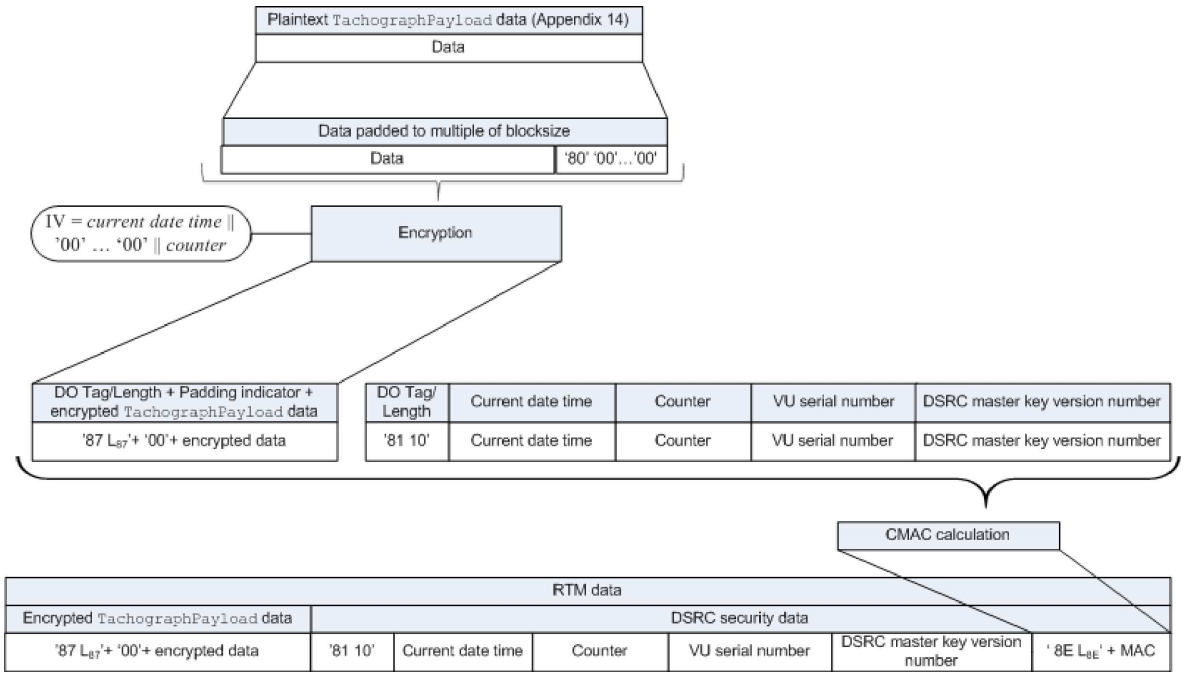
13.2. Cifrado de la carga útil del tacógrafo y generación del código MAC

CSM_226 Dado un elemento de datos de texto plano con el tipo de dato `TachographPayload` descrito en el apéndice 14, una VU cifrará estos datos tal como muestra la Figure 12: la clave DSRC de la VU para el cifrado $K\_VU_{DSRC}\_ENC$ (véase la sección 9.2.2) se usará con el algoritmo AES en el modo de operación de encadenamiento de bloques de cifrado (CBC), tal como se define en la norma [ISO 10116], con un parámetro interpolar $m = 1$. El vector de inicialización será igual a $V =$ *current date time* || *'00 00 00 00 00 00 00 00'* || *counter*, donde *current date time* y *counter* se especifican en CSM_224. Los datos que se deban cifrar se rellenarán por el método 2 definido en la norma [ISO 9797-1].

CSM_227 Una VU calculará el código MAC en los datos de seguridad DSRC como se indica en la Figure 12: el MAC se calculará a través de todos los bytes anteriores en los datos RTM, hasta el número de versión de la clave maestra DSRC, este incluido, e incluyendo las etiquetas y longitudes de los objetos de datos. La VU usará su clave DSRC para comprobar la autenticidad de $K\_VU_{DSRC}\_MAC$ (véase la sección 9.2.2) con el algoritmo AES en modo CMAC, tal como se especifica en la publicación especial [SP 800-38B]. La longitud del código MAC estará relacionada con la longitud de las claves DSRC específicas de la VU, tal como se especifica en CSM_50.

Figura 12

Cifrado de la carga útil del tacógrafo y generación del código MAC



13.3. **Verificación y descifrado de la carga útil del tacógrafo**

CSM_228 Cuando un interrogador remoto reciba datos RTM de una VU, enviará la totalidad de los datos RTM a una tarjeta de control en el campo datos de un comando PROCESS DSRC MESSAGE, tal como se describe en el apéndice 2. Seguidamente:

1. La tarjeta de control inspeccionará el número de versión de la clave maestra DSRC en los datos de seguridad DSRC. Si la tarjeta de control no conoce la clave maestra DSRC indicada, devolverá un error especificado en el apéndice 2 y abortará el proceso.

2. La tarjeta de control usará la clave maestra DSRC indicada en combinación con el número de serie de la VU en los datos de seguridad DSRC para derivar las claves DSRC K_VU_{DSRC}_ENC y K_VU_{DSRC}_MAC específicas de la VU, tal como se especifica en CSM_124.

3. La tarjeta de control usará la clave K_VU_{DSRC}_MAC para verificar el código MAC en los datos de seguridad DSRC, tal como se especifica en CSM_227. Si el código MAC es incorrecto, la tarjeta de control devolverá un error especificado en el apéndice 2 y abortará el proceso.

4. La tarjeta de control usará la clave K_VU_{DSRC}_ENC para descifrar la carga útil cifrada del tacógrafo, tal como se especifica en CSM_226. La tarjeta de control eliminará el relleno y devolverá los datos de la carga útil descifrada al interrogador remoto.

CSM_229 A fin de impedir los ataques por repetición, el interrogador remoto verificará la actualidad de los datos RTM comprobando que la *current date time* de los datos de seguridad DSRC no se desvíe demasiado de la hora actual del interrogador remoto.

Notas:

— Esto exige que el interrogador remoto tenga una fuente exacta y fiable de la hora.

— Puesto que el apéndice 14 exige a una VU que calcule un conjunto de datos RTM nuevo cada 60 segundos, y que se permite que el reloj de la VU se desvíe un minuto de la hora real, un límite inferior de la actualidad de los datos RTM es 2 minutos. La actualidad real exigida depende asimismo de la exactitud del reloj del interrogador remoto.

CSM_230 Cuando un taller verifique el funcionamiento correcto de la funcionalidad DSRC de una VU, enviará la totalidad de los datos RTM recibidos de la VU a una tarjeta de taller en el campo datos de un comando PROCESS DSRC MESSAGE, tal como se describe en el apéndice 2. La tarjeta de taller efectuará todas las comprobaciones y acciones especificadas en CSM_228.

14. FIRMA DE DESCARGAS DE DATOS Y VERIFICACIÓN DE FIRMAS

14.1. **Generalidades**

CSM_231 El equipo dedicado inteligente (IDE) almacenará en un archivo físico los datos recibidos de una VU o de una tarjeta durante una sesión de descarga. Los datos se pueden almacenar en un ESM (medio de almacenamiento externo). El archivo contiene firmas digitales de bloques de datos, tal y como se especifica en el apéndice 7, apartado Protocolos de transferencia de datos. Este archivo contendrá además los certificados siguientes (remítase a la sección 9.1).

— En el caso de una descarga de una VU:

— El certificado VU_Sign

— El certificado MSCA_VU-EGF que contiene la clave pública que deberá utilizarse para la verificación del certificado VU_Sign.

— En el caso de una descarga de una tarjeta:

— El certificado Card_Sign.

— El certificado MSCA_Card que contiene la clave pública que deberá utilizarse para la verificación del certificado Card_Sign.

CSM_232 El IDE dispondrá asimismo de:

— En el caso de que utilice la tarjeta de control para verificar la firma, tal como muestra la Figure 13: El certificado de enlace que relaciona el certificado EUR más reciente con el certificado EUR cuyo período de validez es el directamente anterior, si existe.

— En el caso de que verifique la firma él mismo. todos los certificados raíz europeos válidos.

Nota: el método que el IDE utiliza para recuperar estos certificados no se especifica en el presente apéndice.

14.2. **Generación de firmas**

CSM_233 El algoritmo de firma para crear firmas digitales en datos descargados será el algoritmo ECDSA, tal como se especifica en la norma [DSS], utilizando el algoritmo hash relacionado con el tamaño de clave de la VU o de la tarjeta, tal como se especifica en CSM_50. El formato de la firma será de texto plano, tal como se especifica en la directriz técnica [TR-03111].

14.3. **Verificación de firmas**

CSM_234 Un IDE puede efectuar por sí mismo la verificación de una firma en los datos descargados o utilizar una tarjeta de control a tal efecto. En el caso de que utilice la tarjeta de control, la verificación de la firma se efectuará tal como muestra la Figure 13. En el caso de que efectúe la verificación de la firma por sí mismo, el IDE verificará la autenticidad y validez de todos los certificados de la cadena de certificados en el archivo de datos y verificará asimismo la firma en los datos de acuerdo con el esquema de firma definido en la norma [DSS].

Notas de la Figure 13:

— El equipo que firmó los datos que han de analizarse se denota EQT.

— Los certificados EQT y las claves públicas mencionados en la figura son los empleados para la firma, es decir, VU_Sign o Card_Sign.

— Los certificados EQT.CA y las claves públicas mencionados en la figura son los empleados para firmar los certificados VU o Card, según corresponda.

— El certificado EQT.CA.EUR mencionado en la figura es el certificado raíz europeo indicado en la referencia CAR del certificado EQT.CA.

— El certificado EQT.Link mencionado en la figura es el certificado de enlace del EQT, si está presente. Tal como se especifica en la sección 9.1.2, este es el certificado de enlace para un nuevo par de claves raíz europeo creado por la ERCA y firmado con la clave privada europea anterior.

— El certificado EQT.Link.EUR es el certificado raíz europeo indicado en la referencia CAR del certificado EQT.Link.

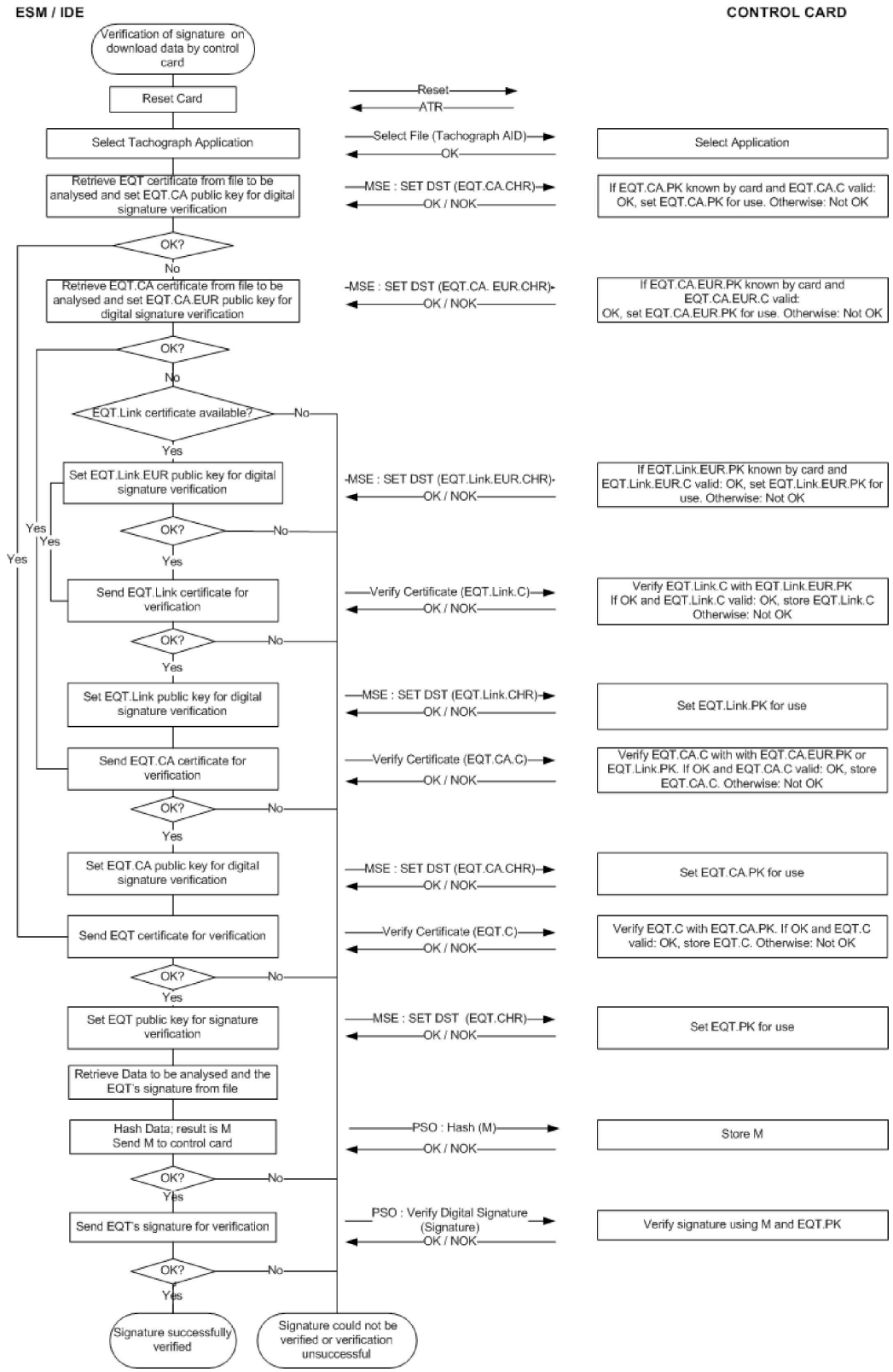
CSM_235 Para calcular la función hash del mensaje M enviada a la tarjeta de control en el comando PSO: Hash, el IDE utilizará el algoritmo hash relacionado con el tamaño de clave de la VU o de la tarjeta de la que se descarguen los datos, tal como se especifica en CSM_50.

CSM_236 Para verificar la firma del EQT, la tarjeta de control seguirá el esquema de firma definido en la norma [DSS].

Nota: El presente documento no especifica ninguna acción que se deba emprender si la firma en un archivo de datos descargado no se puede verificar o si la verificación no se efectúa correctamente.

Figura 13

Protocolo para la verificación de la firma en un archivo de datos descargado.



Apéndice 12

POSICIONAMIENTO BASADO EN EL SISTEMA MUNDIAL DE NAVEGACIÓN POR SATÉLITE (GNSS)

ÍNDICE

1. INTRODUCCIÓN

El presente apéndice recoge los requisitos técnicos para los datos del GNSS empleados por la unidad instalada en el vehículo, incluidos los protocolos que deben aplicarse para garantizar una transferencia de datos segura y correcta de la información sobre el posicionamiento.

Los principales artículos del Reglamento (UE) nº 165/2014 que regulan estos requisitos son: el artículo 8 (Registro de la posición del vehículo en determinados puntos durante el período de trabajo diario), el artículo 10 (Interfaz con sistemas de transporte inteligentes) y el artículo 11 (Disposiciones específicas sobre los tacógrafos inteligentes).

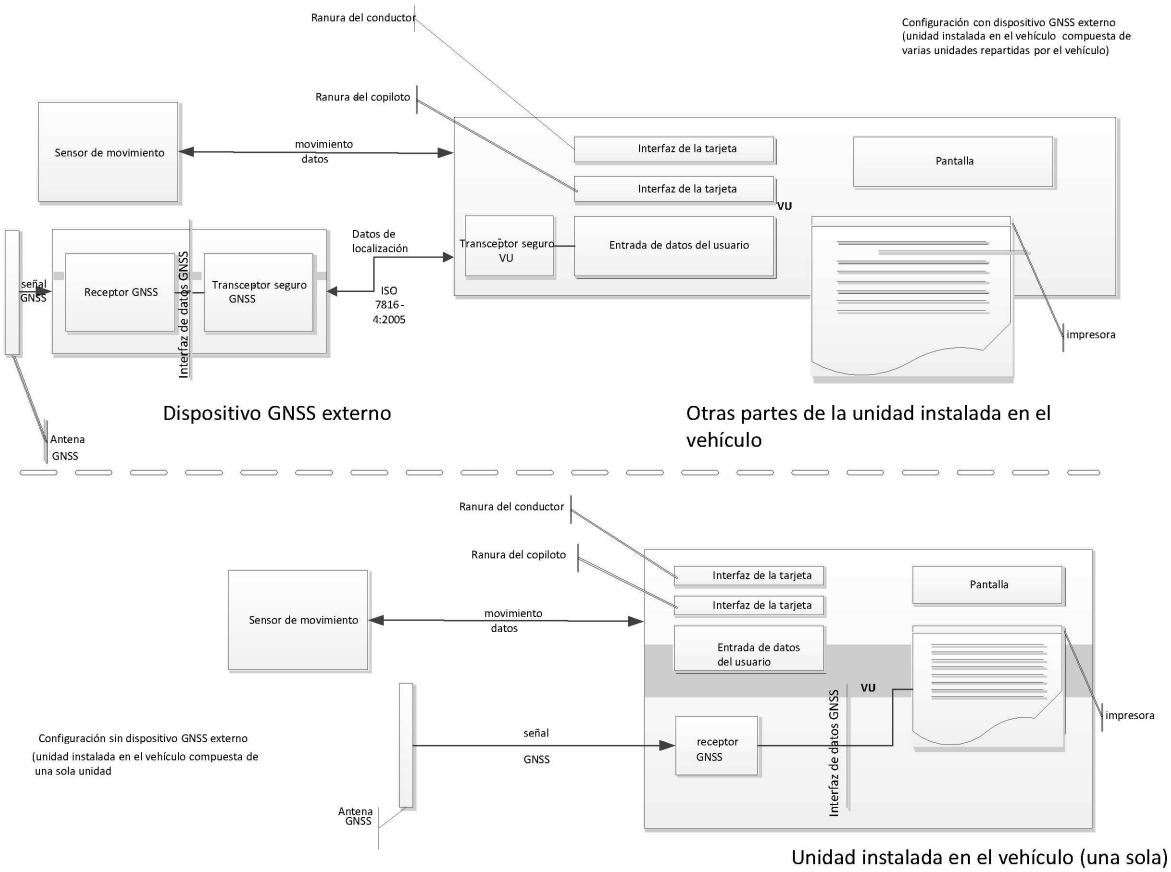
1.1. Ámbito de aplicación

GNS_1 La unidad instalada en el vehículo recabará datos de posición de al menos un GNSS para respaldar la aplicación del artículo 8.

La unidad instalada en el vehículo podrá incluir o no un dispositivo GNSS externo, tal y como se indica en el Gráfico 1:

Gráfico 1

Diferentes configuraciones del receptor GNSS.



1.2. Acrónimos y notaciones

En el presente apéndice se utilizan los siguientes acrónimos:

DOP dilución de precisión

EGF archivo elemental del dispositivo GNSS

EGNOS Sistema Europeo de Navegación por Complemento Geoestacionario

GNSS sistema mundial de navegación por satélite

GSA dilución de precisión del GPS y satélites activos

HDOP dilución de precisión horizontal

ICD documento de control de interfaces

NMEA National Marine Electronics Association

PDOP dilución de precisión de la posición

RMC específico mínimo recomendado

SIS señal en el espacio

VDOP dilución de precisión vertical

VU unidad instalada en el vehículo

2. REQUISITOS DEL RECEPTOR GNSS

Independientemente de la configuración del tacógrafo inteligente, que puede incluir o no un dispositivo GNSS externo, la facilitación de información de posición precisa y fiable es un elemento esencial para el funcionamiento efectivo del tacógrafo inteligente. Por consiguiente, conviene exigir su compatibilidad con los servicios prestados por los programas Galileo y Sistema Europeo de Navegación por Complemento Geoestacionario (EGNOS), con arreglo a lo establecido en el Reglamento (UE) nº 1285/2013 del Parlamento Europeo y del Consejo ([1]). El sistema establecido en el marco del programa Galileo es un sistema mundial independiente de radionavegación por satélite, y el establecido en el marco del programa EGNOS es un sistema regional de navegación por satélite que mejora la calidad de la señal del Sistema de Posicionamiento Global (GPS).

GNS_2 Los fabricantes se asegurarán de que los receptores GNSS integrados en los tacógrafos inteligentes sean compatibles con los servicios de localización prestados por los sistemas Galileo y EGNOS. Además, los fabricantes podrán optar por la compatibilidad con otros sistemas de navegación por satélite.

GNS_3 El receptor GNSS deberá poder admitir la autenticación en la interfaz abierta de Galileo cuando el sistema Galileo facilite dicha interfaz, y cuando la admitan los fabricantes del receptor GNSS.

3. SECUENCIAS DE LA NMEA

En la presente sección se describen las secuencias NMEA utilizadas para el funcionamiento del tacógrafo inteligente. Esta sección es aplicable tanto a la configuración de tacógrafo inteligente con dispositivo GNSS externo como sin él.

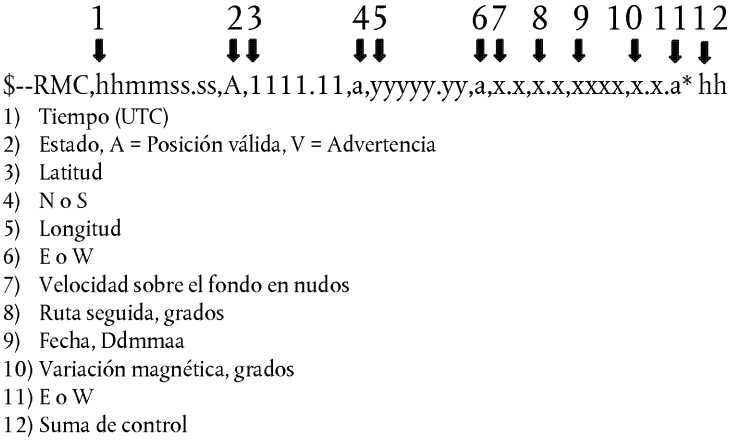
GNS_4 Los datos de localización se basan en los datos específicos mínimos recomendados (RMC) del GNSS recogidos en la secuencia NMEA, que incluyen la información sobre la posición (latitud y longitud), el tiempo en formato UTC (hhmmss.ss) y la velocidad sobre el fondo en nudos, además de valores adicionales.

El formato de la secuencia RMC es el siguiente (según la norma NMEA V4.1):

([1]) Reglamento (UE) nº 1285/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, relativo al establecimiento y la explotación de los sistemas europeos de radionavegación por satélite y por el que se derogan el Reglamento (CE) no 876/2002 del Consejo y el Reglamento (CE) nº 683/2008 del Parlamento Europeo y del Consejo (DO L 347 de 20.12.2013, p. 1).

Gráfico 2

Estructura de la secuencia RMC



El estado indica si se dispone de señal GNSS. Los datos recibidos (por ejemplo, tiempo o latitud/longitud) únicamente podrán utilizarse para registrar la posición del vehículo de la unidad instalada en el vehículo cuando el estado tenga «A» como valor.

La resolución de la posición se basa en el formato de la secuencia RMC anteriormente descrita. La primera parte de los campos 3 y 5 (los dos primeros números) sirve para representar los grados. El resto se emplea para representar los minutos con tres decimales. Por consiguiente, la resolución es de 1/1 000 de minuto o 1/60 000 de grado (puesto que un minuto es 1/60 de un grado).

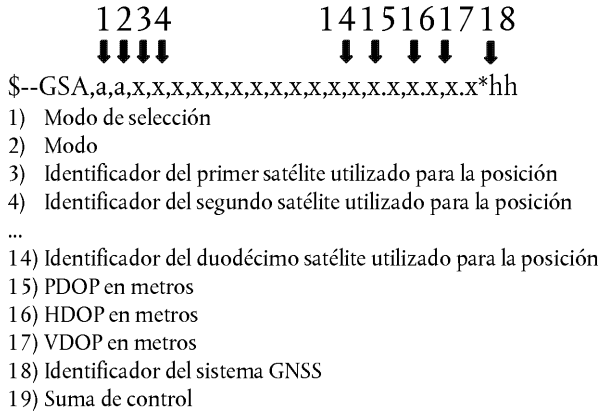
GNS_5 La unidad instalada en el vehículo almacenará en su base de datos la información de posición relativa a la latitud y a la longitud con una resolución de 1/10 de minuto o 1/600 de grado, tal y como se describe en el apéndice 1 para las geocoordenadas.

La VU puede utilizar el comando DOP del GPS y satélites activos (GSA) para definir y registrar la disponibilidad y la precisión de la señal. En concreto, la HDOP se emplea para facilitar una indicación del nivel de precisión de los datos de localización registrados (véase el apartado 4.2.2). La VU almacenará el valor de la HDOP calculado como el mínimo de los valores HDOP recogidos en los sistemas GNSS disponibles.

El identificador de sistema GNSS indica si se trata de GPS, Glonass, Galileo, Beidou o sistema de aumentación basado en satélites (SBAS).

Gráfico 3

Estructura de la secuencia GSA



El modo (2) indica si no se dispone de posición (modo=1), si se dispone de una posición 2D (modo=2) o si se dispone de una posición 3D (modo=3).

GNS_6 La secuencia *GSA* se almacenará con el número de registro «06».

GNS_7 El tamaño máximo de las secuencias NMEA (por ejemplo, RMC, GSA u otras) empleadas para medir el comando de lectura del registro será de 85 bytes (véase la Tabla 1).

4. UNIDAD INSTALADA EN EL VEHÍCULO CON DISPOSITIVO GNSS EXTERNO

4.1. **Configuración**

4.1.1 *Principales componentes e interfaces*

En esta configuración, el receptor GNSS forma parte de un dispositivo GNSS externo.

GNS_8 Dicho dispositivo debe disponer de una interfaz vehicular específica.

GNS_9 El dispositivo GNSS externo estará formado por los siguientes componentes (véase el Gráfico 4):

a) Un receptor GNSS comercial que facilite los datos de posición a través de la interfaz de datos GNSS. Por ejemplo, la interfaz de datos GNSS puede corresponder a la norma NMEA V4.10, de modo que el receptor GNSS actúe como emisor y transmita secuencias NMEA al transceptor seguro GNSS con una frecuencia de 1 Hz para el conjunto predefinido de secuencias NMEA, que debe incluir al menos las secuencias RMC y GSA. Serán los fabricantes del dispositivo GNSS externo quienes decidan aplicar la interfaz de datos GNSS.

b) Una unidad transmisora receptora (transceptor seguro GNSS) con capacidad para respetar la norma ISO/IEC 7816-4:2013 (véase el apartado 4.2.1), comunicarse con la unidad instalada en el vehículo y admitir la interfaz de transferencia de datos GNSS al receptor GNSS. La unidad dispone de una memoria para almacenar los datos identificativos del receptor GNSS y del dispositivo GNSS externo.

c) Un sistema de cierre con un detector de manipulaciones que incluya tanto el receptor GNSS como el transceptor seguro GNSS. El detector de manipulaciones deberá aplicar las medidas de protección de la seguridad solicitadas en el perfil de protección del tacógrafo inteligente.

d) Una antena GNSS instalada en el vehículo y conectada al receptor GNSS mediante el sistema de cierre.

GNS_10 El dispositivo GNSS externo tiene al menos las siguientes interfaces externas:

a) la interfaz de la antena GNSS instalada en el maletero del vehículo, en caso de que se utilice una antena externa; y

b) la interfaz de la unidad instalada en el vehículo.

GNS_11 En la unidad instalada en el vehículo, el transceptor seguro de la VU es el otro fin de la comunicación segura con el transceptor seguro del GNSS, y debe respetar la norma ISO/IEC 7816-4:2013 para la conexión con el dispositivo GNSS externo.

GNS_12 Para el nivel físico de la comunicación con el dispositivo GNSS externo, la unidad instalada en el vehículo respetará la norma ISO/IEC 7816-12:2005 y otras normas que respeten la ISO/IEC 7816-4:2013. (véase el apartado 4.2.1).

4.1.2 *Estado del dispositivo GNSS externo al final de la producción*

GNS_13 El dispositivo GNSS externo deberá almacenar los siguientes valores en la memoria permanente del transceptor seguro del GNSS cuando salga de la fábrica:

— la pareja de claves EGF_MA y el certificado correspondiente;

— el certificado MSCA_VU-EGF que contenga la clave pública MSCA_VU-EGF.PK que se utilizará para verificar el certificado EGF_MA;

— el certificado EUR que contenga la clave pública EUR.PK que se utilizará para verificar el certificado MSCA_VU-EGF;

— el certificado EUR cuyo período de validez finalice exactamente antes del período de validez del certificado EUR empleado para verificar el certificado MSCA_VU-EGF, en caso de que exista;

— el certificado de enlace que vincule estos dos certificados EUR, en caso de que exista;

— el número de serie ampliado del dispositivo GNSS externo;

— el identificador del sistema operativo del dispositivo GNSS;

— el número de homologación del dispositivo GNSS externo; y

— el identificador del componente de seguridad del módulo GNSS externo.

4.2. **Comunicación entre el dispositivo GNSS externo y la unidad instalada en el vehículo**

4.2.1 *Protocolo de comunicación*

GNS_14 El protocolo de comunicación entre el dispositivo GNSS externo y la unidad instalada en el vehículo deberá admitir tres funciones:

1. recogida y distribución de datos GNSS (por ejemplo, posición, tiempo, velocidad);

2. recogida de los datos de configuración del dispositivo GNSS externo; y

3. protocolo de administración para admitir el acoplamiento, la autenticación mutua y el acuerdo de la clave de la sesión entre el dispositivo GNSS externo y la VU.

GNS_15 El protocolo de comunicación se basará en la norma ISO/IEC 7816-4:2013, de modo que el transceptor seguro de la VU actuará como maestro y el transceptor seguro GNSS como esclavo. La conexión física entre el dispositivo GNSS externo y la unidad instalada en el vehículo se basa en la norma ISO/IEC 7816-12:2005 y en otras normas que respeten la norma ISO/IEC 7816-4:2013.

GNS_16 En el protocolo de comunicación no se admitirán campos de longitud ampliada.

GNS_17 El protocolo de comunicación de la norma ISO 7816 (tanto *-4:2013 como *-12:2005) entre el dispositivo GNSS externo y la VU se configurará en T=1.

GNS_18 Para las funciones 1 (recogida y distribución de datos GNSS), 2 (recogida de los datos de configuración del dispositivo GNSS externo) y 3 (protocolo de administración), el transceptor seguro GNSS simulará una tarjeta inteligente con una arquitectura de archivos del sistema formada por: un archivo principal (MF); un archivo de directorio (DF) con el identificador de aplicación especificado en el apéndice 1, apartado 6.2 («FF 44 54 45 47 4D») y con tres EF que contengan certificados; y un archivo elemental único (EF.EGF) con el identificador igual a «2F2F», tal y como se describe en Tabla 1.

GNS_19 El transceptor seguro GNSS almacenará los datos procedentes del receptor GNSS y la configuración en el EF.EGF. Se trata de un archivo de registro lineal y de longitud variable cuyo identificador es «2F2F» en formato hexadecimal.

GNS_20 El transceptor seguro GNSS utilizará una memoria para almacenar los datos que pueda realizar al menos 20 millones de ciclos de escritura/lectura. A excepción de este elemento, el diseño interno y la aplicación del transceptor seguro GNSS queda en manos de los fabricantes.

El mapeado de los números de registro y de los datos se detalla en la Tabla 1. Cabe señalarse que hay cuatro secuencias GSA para los cuatro sistemas satélite y el sistema de aumentación basado en satélites (SBAS).

GNS_21 La Tabla 1 recoge la estructura de los archivos. Para las condiciones de acceso (ALW, NEV, SM-MAC), véase el apéndice 2, apartado 3.5.

Tabla 1

Estructura de los archivos

		Condiciones de acceso		
Archivo	Identificador del archivo	Lectura	Actualización	Cifrado
MF	3F00			
EF.ICC	0002	ALW	NEV (por parte de la VU)	No
DF GNSS Facility	0501	ALW	NEV	No
EF EGF_MACertificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Link_Certificate	C109	ALW	NEV	No
EF.EGF	2F2F	SM-MAC	NEV (por parte de la VU)	No

Archivo/elemento de dato	Nº de registro	Tamaño (bytes)		Valores por defecto
		Mín.	Máx.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS Facility		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
Secuencia RMC NMEA	01	85	85	
Primera secuencia GSA NMEA	02	85	85	
Segunda secuencia GSA NMEA	03	85	85	

Archivo/elemento de dato	Nº de registro	Tamaño (bytes)		Valores por defecto
		Mín.	Máx.	
Tercera secuencia GSA NMEA	04	85	85	
Cuarta secuencia GSA NMEA	05	85	85	
Quinta secuencia GSA NMEA	06	85	85	
Número de serie ampliado del dispositivo GNSS externo definido en el apéndice 1 como sensorSerialNumber.	07	8	8	
Identificador del sistema operativo del transceptor seguro GNSS definido en el apéndice 1 como SensorOSIdentifier.	08	2	2	
Número de homologación del dispositivo GNSS externo definido en el apéndice 1 como SensorExternalGNSSApprovalNumber.	09	16	16	
Identificador del componente de seguridad del dispositivo GNSS externo definido en el apéndice 1 como SensorExternalGNSSSCIdentifier.	10	8	8	
RFU: reservado para uso futuro.	De 11 a FD			

4.2.2 *Transferencia segura de datos GNSS*

GNS_22 Únicamente se permitirá la transferencia segura de datos de posición GNSS en las siguientes condiciones:

1. si se ha llevado a cabo el proceso de acoplamiento tal y como se describe en el apéndice 11 (Mecanismos de seguridad comunes); y

2. si se han realizado con la frecuencia prevista la autenticación mutua periódica y el acuerdo de la clave de la sesión entre la VU y el dispositivo GNSS externo también descritos en el apéndice 11 (Mecanismos de seguridad comunes).

GNS_23 Cada T segundos (siendo T un valor igual o inferior a 10, a menos que se esté realizando el acoplamiento, la autenticación mutua o el acuerdo de la clave de la sesión), la VU solicita al dispositivo GNSS externo información de posición mediante el siguiente proceso:

1. La VU solicita al dispositivo GNSS externo datos de localización y datos sobre la dilución de precisión (de la secuencia GSA NMEA). El transceptor seguro de la VU utilizará el comando de selección y lectura de registros de la ISO/IEC 7816-4:2013 en el modo de solo autenticación de mensajería segura, según lo previsto en el apéndice 11, apartado 11.5, con el identificador de archivo «2F2F» y el número de registro «01» para la secuencia RMC NMEA y «02», «03» ,«04»,«05»,«06» para la secuencia GSA NMEA.

2. Los últimos datos de localización recibidos se almacenan en el EF con el identificador «2F2F», y los registros descritos en la Tabla 1 en el transceptor seguro GNSS, puesto que el transceptor seguro GNSS recibe del receptor GNSS datos NMEA con una frecuencia de al menos 1 Hz a través de la interfaz de datos GNSS.

3. El transceptor seguro GNSS envía la respuesta al transceptor seguro de la VU utilizando un mensaje de respuesta APDU en el modo de solo autenticación de mensajería segura, según lo previsto en el apéndice 11, apartado 11.5.

4. El transceptor seguro de la VU comprueba la autenticidad y la integridad de la respuesta recibida. En caso de que el resultado sea positivo, se transfieren los datos de localización al procesador de la VU a través de la interfaz de datos GNSS.

5. El procesador de la VU verifica los datos recibidos (por ejemplo, latitud, longitud o tiempo) al extraer la información de la secuencia RMC NMEA. La secuencia RMC NMEA incluye la información si la posición es válida. Si la posición no es válida, aún no dispone de datos de localización y no pueden emplearse para registrar la posición del vehículo. Si la posición es válida, el procesador de la VU también extrae los valores de HDOP de las secuencias GSA NMEA y calcula el valor medio en los sistemas de satélite disponibles (es decir, cuando se disponga de una posición).

6. El procesador de la VU almacena en la VU la información recibida y procesada, como la latitud, la longitud, el tiempo y la velocidad, en el formato definido en el diccionario de datos del apéndice 1 como «geocoordenadas», junto con el valor de HDOP calculado como el mínimo de los valores HDOP recogidos en los sistemas GNSS disponibles.

4.2.3 *Estructura del comando de lectura del registro*

En la presente sección se detalla la estructura del comando de lectura del registro (Read Record). Se incluye la mensajería segura (modo de solo autenticación) descrita en el apéndice 11 (Mecanismos de seguridad comunes).

GNS_24 El comando admitirá el modo de solo autenticación de mensajería segura, véase el apéndice 11.

GNS_25 Mensaje de comando

Byte	Longitud	Valor	Descripción
CLA	1	0Ch	Se pide mensajería segura
INS	1	B2h	Lectura del registro
P1	1	XXh	Número de registro («00» se refiere al registro actual)
P2	1	04h	Lectura del registro con el número de registro indicado en P1
Le	1	XXh	Longitud de datos esperada. Número de bytes que se deben leer.

GNS_26 El registro con referencia P1 se convierte en el registro actual.

Byte	Longitud	Valor	Descripción
Nº 1- nº X	X	XX..XXh	Datos leídos
SW	2	XXXXh	Palabras de estado (SW1,SW2)

— Si el comando se ejecuta correctamente, el transceptor seguro GNSS contesta con el estado «**9000**».

— Si el archivo actual no está destinado al registro, el transceptor seguro GNSS contesta con el estado «**6981**».

— Si se utiliza el comando con P1=00 pero no se dispone de EF, el transceptor seguro GNSS contesta con el estado «**6986**» (comando no permitido).

— Si no se localiza el registro, el transceptor seguro GNSS contesta con el estado «**6A 83**».

— Si el dispositivo GNSS externo detecta manipulación, contestará con el estado «**66 90**».

GNS_27 El transceptor seguro GNSS admitirá los siguientes comandos de tacógrafo de segunda generación especificados en el apéndice 2:

Comando	Referencia
Select (seleccionar)	Apéndice 2, apartado 3.5.1
Read Binary (leer archivo binario)	Apéndice 2, apartado 3.5.2
Get Challenge (obtener interrogación)	Apéndice 2, apartado 3.5.4
PSO: Verify Certificate (realizar operación de seguridad: verificar certificado)	Apéndice 2, apartado 3.5.7
External Authenticate (autenticación externa)	Apéndice 2, apartado 3.5.9
General Authenticate (autenticación general)	Apéndice 2, apartado 3.5.10
MSE:SET	Apéndice 2, apartado 3.5.11

4.3. **Acoplamiento, autenticación mutua y acuerdo de la clave de la sesión entre el dispositivo GNSS externo y la unidad instalada en el vehículo**

El acoplamiento, la autenticación mutua y el acuerdo de la clave de la sesión entre el dispositivo GNSS externo y la unidad instalada en el vehículo se describen en el apéndice 11 (Mecanismos de seguridad comunes), apartado 11.

4.4. **Gestión de errores**

En la presente sección se explica cómo se gestionan y se registran en la VU los posibles errores del dispositivo GNSS externo.

4.4.1 *Error de comunicación con el dispositivo GNSS externo*

GNS_28 Si la VU no consigue comunicarse con el dispositivo GNSS externo acoplado durante más de 20 minutos seguidos, la VU generará y registrará en la VU un incidente de tipo EventFaultType con el valor de la enumeración «53H External GNSS communication fault» (error de comunicación con el dispositivo GNSS externo) y con la hora en que se produzca como marca de tiempo. El incidente se generará exclusivamente si se cumplen las siguientes dos condiciones: a) el tacógrafo inteligente no está en modo calibración y b) el vehículo está en movimiento. En este contexto, se genera un error de comunicación cuando el transceptor seguro de la VU no recibe ningún mensaje de respuesta tras un mensaje de petición enviado según se describe en el apartado 4.2.

4.4.2 *Manipulación de la integridad física del dispositivo GNSS externo*

GNS_29 Si se ha manipulado el dispositivo GNSS externo, el transceptor seguro GNSS borrará toda su memoria, incluido el material criptográfico. Tal y como se describe en GNS_25 y en GNS_26, la VU detectará la manipulación si se ha enviado un mensaje de respuesta con el estado «6690». A continuación, la VU generará un incidente de tipo EventFaultType con la enumeración «55H Tamper detection of GNSS» (detección de manipulación del GNSS).

4.4.3 *Ausencia de información de posición del receptor GNSS*

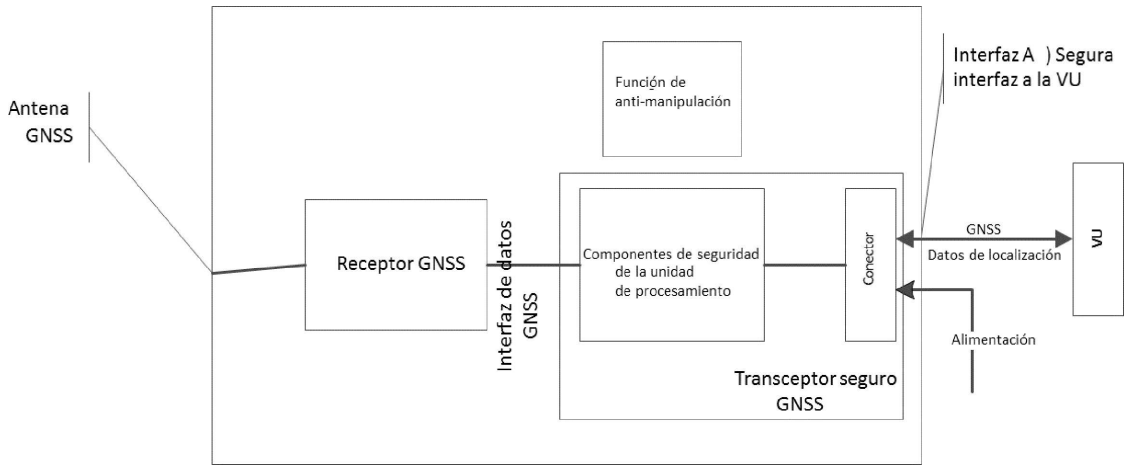
GNS_30 Si el transceptor seguro GNSS no recibe datos del receptor GNSS durante más de tres horas seguidas, el transceptor seguro GNSS generará un mensaje de respuesta con el comando READ RECORD (leer registro) con el número de registro «01» y con un campo de datos de 12 bytes, todos ellos fijados en 0xFF. Una vez recibido el mensaje de respuesta con este valor del campo de datos, la VU solamente generará y registrará un incidente de tipo EventFaultType con la enumeración «52H external GNSS receiver fault» (fallo del receptor GNSS externo) y con la hora en que se produzca como marca de tiempo si se cumplen las siguientes dos condiciones: a) el tacógrafo inteligente no está en modo calibración y b) el vehículo está en movimiento.

4.4.4 *Certificado del dispositivo GNSS externo expirado*

GNS_31 Si la VU detecta que el certificado EGF empleado para las autenticaciones mutuas ya no es válido, generará y registrará un fallo del aparato de control de tipo EventFaultType con la enumeración «56H External GNSS facility certificate expired» (certificado del dispositivo GNSS externo expirado) con la hora en que se produzca como marca de tiempo. La VU seguirá utilizando los datos GNSS de posición recibidos.

Gráfico 4

Esquema del dispositivo GNSS externo



5. UNIDAD INSTALADA EN EL VEHÍCULO SIN DISPOSITIVO GNSS EXTERNO

5.1. Configuración

En esta configuración, el receptor GNSS se encuentra dentro de la unidad instalada en el vehículo, tal y como se refleja en el Gráfico 1.

GNS_32 El receptor GNSS actuará como emisor y transmitirá secuencias NMEA al procesador de la VU, que actuará como receptor con una frecuencia de 1/10 Hz o superior para el conjunto predeterminado de secuencias NMEA, que incluirá como mínimo las secuencias RMC y GSA.

GNS_33 Se conectará a la VU una antena GNSS externa instalada en el vehículo o una antena GNSS interna.

5.2. Gestión de errores

5.2.1 *Ausencia de información de posición del receptor GNSS*

GNS_34 Si la VU no recibe datos del receptor GNSS durante más de tres horas seguidas, solamente generará y registrará un incidente de tipo EventFaultType con la enumeración «51H Internal GNSS receiver fault» (fallo del receptor GNSS interno) y con la hora en que se produzca como marca de tiempo si se cumplen las siguientes dos condiciones: a) el tacógrafo inteligente no está en modo calibración y b) el vehículo está en movimiento.

6. ERROR DE SINCRONIZACIÓN DEL GNSS

Si la VU detecta una discrepancia de más de un minuto entre el tiempo de la función de medición del tiempo de la unidad instalada en el vehículo y el tiempo procedente del receptor GNSS, generará y registrará un incidente de tipo EventFaultType con la enumeración «0BH Time conflict (GNSS versus VU internal clock)» (discrepancia temporal entre el GNSS y el reloj interno de la VU). Se registra el incidente junto con el valor del reloj interno de la unidad instalada en el vehículo y se realiza un ajuste automático de la hora. Cuando se produzca una discrepancia temporal, la VU no comprobará el desajuste hasta pasadas doce horas. Este incidente no se producirá en casos en los que el receptor GNSS no haya detectado una señal GNSS válida en los últimos treinta días. No obstante, cuando se vuelva a disponer de información de posición del receptor GNSS, se realizará el ajuste automático de la hora.

7. CONFLICTO DE MOVIMIENTO DEL VEHÍCULO

GNS_35 La VU producirá y registrará un conflicto de movimiento del vehículo (véase el requisito 84 del anexo), con la hora en que se produzca como marca de tiempo, cuando la información de movimiento calculada por el sensor de movimiento no sea acorde a la información de movimiento calculada por el receptor interno de GNSS o por el dispositivo GNSS externo. Para detectar estas contradicciones se utilizará el valor mediano de las diferencias de velocidad entre estas fuentes, como se indica a continuación:

— cada diez segundos como máximo, se calculará el valor absoluto de la diferencia entre la velocidad del vehículo estimada por el GNSS y la estimada por el sensor de movimiento;

— para calcular el valor mediano se utilizarán todos los valores computados en un intervalo de tiempo que incluya los últimos cinco minutos de movimiento; y

— el valor mediano será la media del 80 % de los valores restantes, después de haberse eliminado los valores absolutos más elevados.

El incidente de conflicto de movimiento del vehículo se producirá si el valor mediano es superior a 10 km/hora durante cinco minutos seguidos en los que el vehículo esté en movimiento. De manera opcional, podrán emplearse otras fuentes independientes de detección de movimiento del vehículo para facilitar una detección más fiable de manipulaciones del tacógrafo. (*Nota:* con el empleo de la mediana de los últimos cinco minutos se pretende mitigar el riesgo de obtener mediciones discrepantes y valores transitorios). Este incidente no se producirá en los siguientes casos: a) durante trayectos en ferri o en tren, b) cuando no se disponga de información de posición del receptor GNSS y c) en modo de calibrado.

Apéndice 13

INTERFAZ ITS

ÍNDICE

1. INTRODUCCIÓN

El presente apéndice especifica el diseño y los procedimientos a seguir para implementar la inferfaz con los sistemas de transporte inteligentes (ITS) de conformidad con lo dispuesto en el artículo 19 del Reglamento (UE) nº 165/2014 (*el Reglamento*).

El Reglamento especifica que los tacógrafos de los vehículos podrán ir equipados de interfaces normalizadas que permitan que los datos registrados o producidos por el tacógrafo se utilicen en modo operativo gracias a un dispositivo externo, siempre que se cumplan las siguientes condiciones:

a) la interfaz no afecte a la autenticidad ni a la integridad de los datos del tacógrafo;

b) la interfaz cumpla las disposiciones específicas del artículo 11;

c) el dispositivo externo conectado con la interfaz tenga acceso a los datos personales, incluso a los datos de geoposicionamiento, únicamente tras el consentimiento verificable del conductor al que se refieran los datos.

2. ÁMBITO DE APLICACIÓN

El ámbito del presente apéndice es especificar la forma en que las aplicaciones alojadas en dispositivos externos pueden obtener datos (*los datos*) de un tacógrafo a través de una conexión Bluetooth®.

Los datos disponibles a través de esta interfaz están descritos en el anexo 1 del presente documento. Esta interfaz no prohíbe la implementación de otras inferfaces (por ejemplo, a través del bus CAN) para transmitir los datos de la VU a otras unidades de procesamiento del vehículo.

Este apéndice expecifica:

— *Los datos* disponibles a través de la interfaz ITS.

— El perfil Bluetooth® utilizado para transferir los datos.

— Los procedimientos de interrogación y descarga y la secuencia de operaciones.

— Los mecanismos de emparejamiento entre el tacógrafo y el dispositivo externo.

— El mecanismo de consentimiento disponible para el conductor.

A efectos de aclaración, el presente anexo no especifica:

— La operación y gestión de la recogida de *los datos* en la VU (que se especificarán en otro punto del *Reglamento*, o que de otra manera serán función del diseño del producto).

— La forma de presentación de los datos recogidos a la aplicación alojada en el dispositivo externo.

— Las disposiciones sobre seguridad de los datos más allá de la proporcionada por Bluetooth® (como el cifrado) en lo que se refiere al contenido de los *datos* [que se especificarán en otro punto del *Reglamento* (apéndice 10, Mecanismos comunes de seguridad)].

— Los procolos Bluetooth® usados por la interfaz ITS.

2.1. **Siglas, definiciones y notaciones**

En este apéndice se utilizan las siguientes siglas y definiciones específicas:

La comunicación	intercambio de información/datos entre una unidad maestra (es decir, los tacógrafos) y una unidad externa a través de la interfaz ITS a través de Bluetooth®.
Los datos	Los conjuntos de datos tal como se especifican en el anexo 1.
El Reglamento	Reglamento (UE) nº 165/2014 del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, relativo a los tacógrafos en el transporte por carretera, por el que se deroga el Reglamento (CEE) nº 3821/85 del Consejo relativo al aparato de control en el sector de los transportes por carretera y se modifica el Reglamento (CE) nº 561/2006 del Parlamento Europeo y del Consejo relativo a la armonización de determinadas disposiciones en materia social en el sector de los transportes por carretera.
BR	Basic Rate (Velocidad básica)
EDR	Enhanced Data Rate (Velocidad de datos mejorada)
GNSS	Global Navigation Satellite System (Sistema mundial de navegación por satélite)
IRK	Identity Resolution Key (Clave de resolución de identidad)
ITS	Sistema de transporte inteligente
LE	Low Energy (Baja energía)
PIN	Personal Identification Number (Número de identificación personal)
PUC	Personal Unblocking Code (Código de desloqueo personal)
SID	Service Identifier (Identificador del servicio)
SPP	Serial Port Profile (Perfil de puerto serie)
SSP	Secure Simple Pairing (Emparejamiento sencillo seguro)
TRTP	Transfer Request Parameter (Parámetro de la petición de transferencia)
TREP	Transfer Response Parameter (Parámetro de la respuesta a la petición de transferencia)
VU	Vehicle Unit (Unidad instalada en el vehículo)

3. REGLAMENTOS Y NORMAS DE REFERENCIA

La especificación definida en el presente apéndice se refiere total o parcialmente a los siguientes Reglamentos y normas, de los que depende. En las cláusulas de este apéndice se especifican las normas pertinentes, o las cláusulas pertinentes de las mismas. En el caso de que surgiera cualquier contradicción, prevalecerán las cláusulas del presente apéndice.

Los Reglamentos y normas a los que se remite el presente apéndice son:

— Reglamento (UE) nº 165/2014 del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, relativo a los tacógrafos en el transporte por carretera, por el que se deroga el Reglamento (CEE) nº 3821/85 del Consejo relativo al aparato de control en el sector de los transportes por carretera y se modifica el Reglamento (CE) nº 561/2006 del Parlamento Europeo y del Consejo relativo a la armonización de determinadas disposiciones en materia social en el sector de los transportes por carretera.

— Reglamento (CE) nº 561/2006 del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, relativo a la armonización de determinadas disposiciones en materia social en el sector de los transportes por carretera y por el que se modifican los Reglamentos (CEE) nº 3821/85 y (CE) nº 2135/98 del Consejo y se deroga el Reglamento (CEE) nº 3820/85 del Consejo.

— ISO 16844 — 4: Vehículos de carretera — Sistemas de tacógrafo — Parte 4: Interfaz CAN

— ISO 16844 — 7: Vehículos de carretera — Sistemas de tacógrafo — Parte 7: Parámetros

— Bluetooth® — Perfil de puerto serie — V1.2

— Bluetooth® — Versión Core 4.2

— Protocolo NMEA 0183 V4.1

4. PRINCIPIOS DE FUNCIONAMIENTO DE LA INTERFAZ

4.1. **Condiciones previas para la transferencia de datos a través de la interfaz ITS**

La VU será responsable de actualizar y mantener los datos que se deban almacenar en la VU sin ninguna participación de la interfaz ITS. El medio para ello está situado en el interior de la VU, se especifica en otros puntos del Reglamento y no se especifica en el presente apéndice.

4.1.1 *Datos facilitados a través de la interfaz ITS*

La VU será responsable de actualizar los datos que estarán disponibles a través de la interfaz ITS con una frecuencia determinada en los procedimientos de la VU, sin ninguna participación de su interfaz ITS. Los datos de la VU servirán de base para poblar y actualizar los *datos*, el medio para ello se especifica en otros puntos del Reglamento o, si no existe tal especificación, es una función del diseño del producto y no se especifica en el presente apéndice.

4.1.2 *Contenido de los datos*

El contenido de los *datos* será el especificado en el anexo 1 del presente apéndice.

4.1.3 *Aplicaciones ITS*

Las aplicaciones ITS utilizarán los datos puestos a disposición a través de la interfaz ITS, por ejemplo para optimizar la gestión de las actividades del conductor dentro del respeto del Reglamento, para detectar posibles fallos del tacógrafo o para usar los datos del GNSS. La especificación de las aplicaciones no está en el ámbito del presente apéndice.

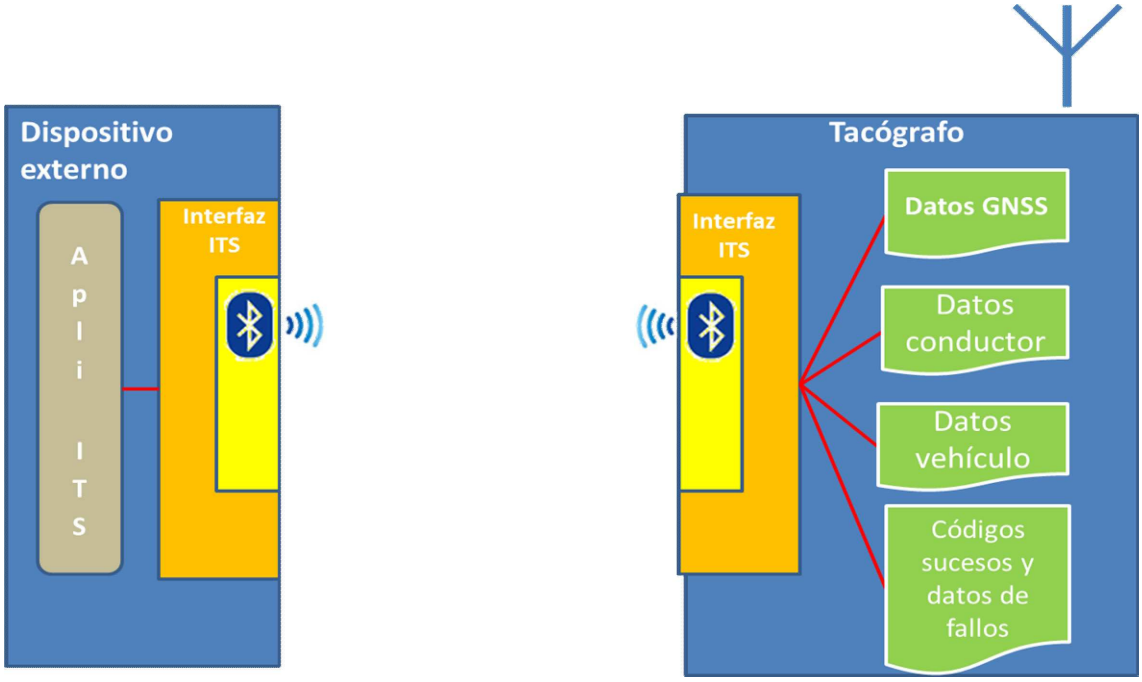
4.2. **Tecnología de la comunicación**

El intercambio de *datos* mediante la interfaz ITS se efectuará a través de una interfaz Bluetooth® compatible de versión 4.2 o posterior. Bluetooth® opera en la banda industrial, científica y médica (ISM) sin licencia a entre 2,4 y 2,485 GHz. Bluetooth® 4.2 ofrece mecanismos de privacidad y seguridad mejoradas y aumenta la velocidad y fiabilidad de las transferencias de datos. A efectos de esta especificación, se utiliza Bluetooth® de clase 2 con un alcance de la señal de hasta 10 metros. Para mayor información sobre Bluetooth® 4.2, consúltese www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

La *comunicación* se establecerá con el equipo de comunicaciones después de efectuado un proceso de emparejamiento por parte de un dispositivo autorizado. Puesto que Bluetooth® utiliza un modelo maestro/esclavo para controlar el momento y el lugar en que los dispositivos pueden enviar datos, el tacógrafo tendrá la función de maestro, mientras que el dispositivo externo tendrá la de esclavo.

Cuando un dispositivo externo entra dentro del radio de alcance de la VU por primera vez, puede iniciarse el proceso de emparejamiento de Bluetooth® (véase también el anexo 2). Los dispositivos comparten sus direcciones, nombres y perfiles y clave secreta común, que les permite conectarse cada vez que entren en contacto en el futuro. Una vez finalizado este paso, el dispositivo externo es de confianza y está en situación de iniciar solicitudes de descarga de datos del tacógrafo. No está previsto añadir mecanismos de cifrado más allá de los facilitados por Bluetooth®. No obstante, si se necesitan mecanismos de seguridad adicionales se proedrá de conformidad con el lo establecido en el apéndice 10 Mecanismos comunes de seguridad.

La figura siguiente muestra el principio general de la comunicación.



El perfil SPP (perfil de puerto serie) de Bluetooth® servirá para transferir datos de ña VU al dispositivo externo.

4.3. **Autorización mediante PIN**

Por razones de seguridad, la VU aplicará un sistema de autorización mediante código PIN separado del emparejamiento Bluetooth. Cada VU será capaz de generar códigos PIN con fines de autenticación compuestos de al menos 4 cifras. Cada vez que un dispositivo externo se empareje con la VU deberá introducir el código PIN correcto antes de recibir datos.

Si introduce el PIN correcto, el dispositivo pasa a la lista blanca que almacenará al menos 64 dispositivos emparejados con una VU específica.

Un dispositivo que no consiga introducir el código PIN correcto tres veces seguidas pasará temporalmente a la lista negra. Mientras el dispositivo siga en la lista negra, toda nueva tentativa de emparejamiento será rechazada. Cada nuevo intento fallido tres veces seguidas de introducción del código PIN correcto tendrá como consecuencia una prohibición de cada vez mayor duración (véase la tabla 1). La introducción del código PIN correcto reajustará la duración de la prohibición y el número de intentos. La figura 1 del anexo 2 representa el diagrama de secuencia de un intento de validación de un código PIN.

Tabla 1

Duración de la prohibición según el número de intentos fallidos consecutivos de introducción del código

Número de fallos consecutivos	Duración de la prohibición
3	30 segundos
6	5 minutos
9	1 hora
12	24 horas
15	Permanente

Una unidad ITS que no consiga introducir el código PIN correcto quince veces (5 × 3) seguidas pasará permanentemente a la lista negra. La prohibición permanente solamente podrá anularse introduciendo el código PUC correcto.

El código PUC estará compuesto de 8 cifras y será facilitado por el fabricante junto con la VU. Una unidad ITS que no consiga introducir el código PUC correcto diez veces seguidas pasará irrevocablemente a la lista negra.

Si bien el fabricante puede ofrecer la opción de cambiar el código PIN directamente a través de la VU, el código PUC no será modificable. La modificación del código PIN, si es posible, exigirá la introducción del código PIN actual directamente en la VU.

Además, los dispositivos almacenados en la lista blanca se mantendrán hasta que el usuario los elimine manualmente (por ejemplo, a través de la interfaz hombre-máquina de la VU u otro medio). De este modo pueden eliminarse de la lista blanca las unidades ITS perdidas o robadas. Por otra parte, las unidades ITS que salgan fuera del radio de alcance de la conexión Bluetooth durante más de 24 horas serán automáticamente eliminadas de la lista blanca de la VU y deberán presentar de nuevo el código PIN correcto al restablecer la conexión.

El formato de los mensajes entre la interfaz de la VU y la VU no se facilita, sino que se deja a la discreción del fabricante. No obstante, el fabricante deberá asegurar que se respete el formato de los mensajes entre la unidad ITS y la interfaz de la VU (véase las especificaciones de la norma ASN.1).

Antes que una solicitud de datos reciba cualquier tipo de tratamiento, se verificarán las credenciales del remitente. La figura 2 del anexo 2 representa el diagrama de secuencia de este procedimiento. Los dispositivos que estén en la lista negra recibirán un rechazo automático, mientras que los dispositivos que no estén ni en la lista negra ni en la lista blanca recibirán una solicitud de PIN a la que deberán responder antes de volver a enviar su solicitud de datos.

4.4. **Formato de los mensajes**

Todos los mensajes que intercambien la unidad ITS y la interfaz de la VU presentarán una estructura con un formato compuesto de tres partes: Una cabecera compuesta de un byte objetivo (TGT), un byte fuente (SRC) y un byte de longitud (LEN).

El campo de datos se compone de un byte identificador de servicio (SID) y una cantidad variable de bytes de datos (máximo 255).

El byte de suma de control es la suma de de todos los bytes del mensaje tomados de 1 byte en 1 byte, en módulo 256, excluido el propio CS.

El mensaje será Big Endian.

Tabla 2

Formato general del mensaje

Cabecera			Campos de datos					Suma de control
TGT	SRC	LEN	SID	TRTP	CC	CM	DATOS	CS
3 bytes			Máx. 255 bytes					1 byte

Cabecera

TGT y SRC: el ID de los dispositivos objetivo (TGT) y fuente (SRC) del mensaje. La interfaz de la VU tendrá el ID por defecto «EE». Este ID no se puede cambiar. La unidad ITS utilizará el ID por defecto «A0» para su primer mensaje de la sesión de comunicación. Seguidamente, la interfaz de la VU asignará un ID único a la unidad ITS, a la que informará del mencionado ID para futuros mensajes durante la sesión.

El byte LEN solamente tendrá en cuenta la parte «DATOS» del campo de datos (véase la tabla 2), los 4 primeros bytes son implícitos.

La interfaz VU confirmará la autenticidad del remitente del mensaje cruzando su propia lista ID con los datos Bluetooth comprobando que la unidad ITS enumerada en el ID facilitado está actualmente dentro del radio de alcance de la conexión Bluetooth.

Campo de datos

Además del SID, el campo de datos contendrá asimismo otros parámetros: un parámetro de petición de transparencia (TRTP) y bytes de contador.

Si los datos que hay que transportar son más largos que el espacio disponible en un mensaje, se dividirán entre varios submensajes. Cada submensaje tendrá la misma cabecera y SID, pero contendrá un contador de 2 bytes, Counter Current (CC) y Counter Max (CM), para indicar el número de submensajes. Al objeto de permitir la verificación de errores y la cancelación, el dispositivo receptor confirma cada uno de los submensajes. El dispositivo de recepción puede aceptar el submensaje, solicitar su retransmisión, pedir al dispositivo de envío que comience de nuevo o abortar la transmisión.

Si no se utilizan, el CC y el CM recibirán el valor 0xFF.

Por ejemplo, el mensaje siguiente

HEADER	SID	TRTP	CC	CM	DATOS	CS
3 bytes	Más largo de 255 bytes					1 byte

Se transmitirá de este modo:

HEADER	SID	TRTP	01	n	DATA	CS
3 bytes	255 bytes					1 byte

HEADER	SID	TRTP	02	n	DATA	CS
3 bytes	255 bytes					1 byte

…

HEADER	SID	TRTP	N	N	DATA	CS
3 bytes	Máx. 255 bytes					1 byte

La tabla 3 contiene los mensajes que la VU y la unidad ITS podrán intercambiar. El contenido de cada parámetro se da en hexadecimal. En aras de la claridad, el CC y el CM no están representados en la tabla, véase la tabla anterior para el formato completo.

Tabla 3

Contenido detallado del mensaje

Mensaje	Cabecera			DATOS			Suma de control
	TGT	SRC	LEN	SID	TRTP	DATOS	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Tiempo	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		

Mensaje	Cabecera			DATOS			Suma de control
	TGT	SRC	LEN	SID	TRTP	DATOS	
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Datos	
DataUnavailable							
Datos no disponibles	*ITSID*	EE	02	0A	TREP	10	
Datos personales no compartidos	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Envío no aceptado	*ITSID*	EE	02	0 B	SID pet.	10	
Servicio no admitido	*ITSID*	EE	02	0 B	SID pet.	11	
Subfunción no admitida	*ITSID*	EE	02	0 B	SID pet.	12	
Longitud del mensaje incorrecta	*ITSID*	EE	02	0 B	SID pet.	13	
Condiciones incorrectas o error en la secuencia de la petición	*ITSID*	EE	02	0 B	SID pet.	22	
Petición no admisible	*ITSID*	EE	02	0 B	SID pet.	31	
Datos no disponibles	*ITSID*	EE	02	0 B	SID pet.	78	
Discordancia ITSID	*ITSID*	EE	02	0 B	SID pet.	FC	
ITSID No encontrado	*ITSID*	EE	02	0 B	SID pet.	FB	

RequestPIN (SID 01)

La interfaz de la VU envía este mensaje si una unidad ITS que no está en la lista negra, pero tampoco en la blanca, envía una petición de datos.

SendITSID (SID 02)

La interfaz de la VU envía este mensaje siempre que un nuevo dispositivo envíe una petición. Este dispositivo usará el ID por defecto «A0» antes de recibir un ID único para la sesión de comunicación.

SendPIN (SID 03)

La unidad ITS envía este mensaje para que la interfaz de la VU lo incluya en su lista blanca. El contenido de este mensaje es un código de 4 ENTEROS entre 0 y 9.

PairingResult (SID 04)

La interfaz de la VU envía este mensaje para informar a la unidad ITS de si el código PIN enviado era el correcto. El contenido de este mensaje será un BOOLEANO con el valor «verdadero» si el código PIN era correcto, y «falso» de lo contrario.

SendPUC (SID 05)

La unidad ITS envía este mensaje para levantar una sanción de inclusión en la lista negra de la interfaz de la VU. El contenido de este mensaje es un código de 8 ENTEROS entre 0 y 9.

BanLiftingResult (SID 06)

La interfaz de la VU envía este mensaje para informar a la unidad ITS de si el código PUC enviado era el correcto. El contenido de este mensaje será un BOOLEANO con el valor «verdadero» si el código PUC era correcto, y «falso» de lo contrario.

RequestRejected (SID 07)

La interfaz de la VU envía este mensaje en respuesta a cualquier mensaje de una unidad ITS incluida en la lista negra, salvo «SendPUC». El mensaje contendrá el tiempo restante que la unidad ITS esté incluida en la lista negra de acuerdo con el formato de la secuencia «Hora» definida en el anexo 3.

RequestData (SID 08)

La unidad ITS envía este mensaje para acceder a datos. Un parámetro de petición de transferencia (TRTP) de un byte indica el tipo de datos solicitados. Existen varios tipos de datos:

— standardTachData (TRTP 01): Datos disponibles del tacógrafo clasificados como no personales.

— personalTachData (TRTP 02): Datos disponibles del tacógrafo clasificados como personales.

— gnssData (TRTP 03): Datos del GNSS, siempre personales.

— standardEventData (TRTP 04): Datos de suceso registrados clasificados como no personales

— personalEventData (TRTP 05): Datos de suceso registrados clasificados como personales

— standardFaultData (TRTP 06): Fallos registrados clasificados como no personales

— manufacturerData (TRTP 07): datos puestos a disposición por el fabricante.

Véase el anexo 3 del presente apéndice para más información sobre el contenido de cada tipo de dato.

Véase el apéndice 12 para más información sobre el formato y el contenido de los datos del GNSS.

Véanse los anexos IB y IC para más información sobre código de datos de suceso y fallos.

ResquestAccepted (SID 09)

La interfaz de la VU envía este mensaje si se ha aceptado un mensaje «RequestData» de la unidad ITS. Este mensaje contiene un TREP de 1 byte, que es el byte TRTP del mensaje «RequestData» asociado, y todos los datos del tipo solicitado.

DataUnavailable (SID 0A)

La interfaz de la VU envía este mensaje si, por una razón determinada, los datos solicitados no están disponibles para ser enviados a una unidad ITS incluida en la lista blanca. El mensaje contiene un TREP de 1 byte que es el TRTP de los datos solicitados y un código de error de 1 byte especificado en la tabla 3. Están disponibles los códigos siguientes:

— No hay datos disponibles (10): La interfaz de la VU no puede acceder a los datos de la VU por razones no especificadas.

— Datos personales no compartidos (11): La unidad ITS intenta recuperar datos personales cuando no son compartidos.

NegativeAnswer (SID 0B)

La interfaz de la VU envía estos mensajes si no puede efetuarse una petición por cualquier otra razón que la indisponibilidad de los datos. Normalmente estos mensajes son el resultado de un formato de petición incorrecto (Longitud, SID, ITSID...), pero no siempre. El TRTP en el campo de datos contiene el identificador de seguridad SID de la petición. El campo da datos contiene un código que identifica la razón de la respuesta negativa. Están disponibles los códigos siguientes:

— Rechazo general (código: 10)

— Esta acción no puede efectuarse por una razón no citada a continuación ni en la sección (*DataUnavailable*).

— Servicio no admitido (código: 11)

— SID de la petición no comprendido.

— Subfunción no admitida (código: 12)

— TRTP de la petición no comprendido. A causa, por ejemplo, de ausencia de valores aceptados.

— Longitud del mensaje incorrecta (código: 13)

— La longitud del mensaje recibido es incorrecta (discordancia entre el byte LEN y la longitud real del mensaje).

— Condiciones incorrectas o error en la secuencia de la petición (código: 22)

— El servicio requerido no está activo o la secuencia de mensajes de petición es incorrecta.

— Petición no admisible (código: 33)

— El registro del parámetro de la solicitud (campo de datos) no es válido.

— Respuesta pendiente (código: 78)

— La acción solicitada no se puede efectuar a tiempo y la VU no está preparada para aceptar otra petición.

— Discordancia del ITSID (código: FB)

— El SRC *ITSID* no concuerda con el dispositivo asociado tras la comparación con la información Bluetooth.

— *ITSID* no encontrado (código: FC)

— El SRC *ITSID* no está asociado a ningún dispositivo.

Las líneas 1 a 72 (**FormatMessageModule**) del código ASN.1 del anexo 3 especifican el formato de los mensajes tal como se describe en la tabla 3. A continuación figuran más detalles sobre el contenido de los mensajes.

4.5. **Consentimiento del conductor**

Todos los datos disponibles están clasificados como estándar o personales. Los datos personales solo serán accesibles si el conductor dio su consentimiento en aceptar que sus datos de tacógrafo personales puedan salir de la red del vehículo para aplicaciones de terceros.

El conductor da su consentimiento cuando, al introducir por primera vez una tarjeta de conductor o de taller actualmente desconocida para la unidad instalada en el vehículo, se invita al titular de la tarjeta a expresar su consentimiento para la salida de datos personales relacionados con el tacógrafo a través de la interfaz opcional ITS. (véase también el anexo I C, apartado 3.6.2).

El estado de consentimiento (activado/desactivado) se registra en la memoria del tacógrafo.

En el caso de múltiples conductores, solamente se compartirán con la interfaz ITS los datos personales de los conductores que hayan dado su consentimiento. Por ejemplo, si en el vehículo hay dos conductores y solamente el primero ha aceptado compartir sus datos personales, los relativos al segundo conductor no serán compartidos.

4.6. **Recuperación de datos estándar**

La figura 3 del anexo 2 representa los diagramas de secuencia de una petición válida enviada por la unidad ITS para acceder a datos estándar. La unidad ITS figura en la lista blanca y no pide datos personales, no es necesaria ninguna verificación adicional. Los diagramas consideran que ya se ha seguido el procedimiento adecuado ilustrado en la figura 2 del anexo 2. Pueden equipararse a la casilla gris *REQUEST TREATMENT* de la figura 2.

Entre los datos disponibles, se considerarán estándar:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Recuperación de datos personales**

La figura 4 del anexo 2 representa el diagrama de secuencia para el procesamiento de peticiones de datos personales. Como se ha dicho anteriormente, la interfaz VU solamente enviará datos personales si el conductor ha dado su consentimiento explícito (véase también 4.5). De otro modo, la petición deberá ser automáticamente rechazada.

Entre los datos disponibles, se considerarán personales:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Recuperación de datos de incidentes y fallos**

Las unidades ITS deberán poder solicitar datos de incidentes que contengan la lista de todos los incidentes inesperados. Estos datos se considerarán estándar o personales, véase el anexo 3. El contenido de cada incidente deberá ser conforme a la documentación presentada en el anexo 1 de este apéndice.

ANEXO 1

LISTA DE DATOS DISPONIBLES A TRAVÉS DE LA INTERFAZ ITS

Datos	Fuente	Clasificación recomendada
VehicleIdentificationNumber	Unidad Vehículo	**no personal**
CalibrationDate	Unidad Vehículo	**no personal**
TachographVehicleSpeed speed instant t	Unidad Vehículo	personal
Driver1WorkingState Selector driver	Unidad Vehículo	personal
Driver2WorkingState	Unidad Vehículo	personal
DriveRecognize Speed Threshold detected	Unidad Vehículo	**no personal**
Driver1TimeRelatedStates Weekly day time	Tarjeta conductor	personal
Driver2TimeRelatedStates	Tarjeta conductor	personal
DriverCardDriver1	Unidad Vehículo	**no personal**
DriverCardDriver2	Unidad Vehículo	**no personal**
OverSpeed	Unidad Vehículo	personal
TimeDate	Unidad Vehículo	**no personal**
HighResolutionTotalVehicleDistance	Unidad Vehículo	**no personal**
ServiceComponentIdentification	Unidad Vehículo	**no personal**
ServiceDelayCalendarTimeBased	Unidad Vehículo	**no personal**
Driver1Identification	Tarjeta conductor	personal
Driver2Identification	Tarjeta conductor	personal
NextCalibrationDate	Unidad Vehículo	**no personal**
Driver1ContinuousDrivingTime	Tarjeta conductor	personal
Driver2ContinuousDrivingTime	Tarjeta conductor	personal
Driver1CumulativeBreakTime	Tarjeta conductor	personal
Driver2CumulativeBreakTime	Tarjeta conductor	personal
Driver1CurrentDurationOfSelectedActivity	Tarjeta conductor	personal
Driver2CurrentDurationOfSelectedActivity	Tarjeta conductor	personal

Datos	Fuente	Clasificación recomendada
SpeedAuthorised	Unidad Vehículo	**no personal**
TachographCardSlot1	Tarjeta conductor	**no personal**
TachographCardSlot2	Tarjeta conductor	**no personal**
Driver1Name	Tarjeta conductor	personal
Driver2Name	Tarjeta conductor	personal
OutOfScopeCondition	Unidad Vehículo	**no personal**
ModeOfOperation	Unidad Vehículo	**no personal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Tarjeta conductor	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Tarjeta conductor	personal
EngineSpeed	Unidad Vehículo	personal
RegisteringMemberState	Unidad Vehículo	**no personal**
VehicleRegistrationNumber	Unidad Vehículo	**no personal**
Driver1EndOfLastDailyRestPeriod	Tarjeta conductor	personal
Driver2EndOfLastDailyRestPeriod	Tarjeta conductor	personal
Driver1EndOfLastWeeklyRestPeriod	Tarjeta conductor	personal
Driver2EndOfLastWeeklyRestPeriod	Tarjeta conductor	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Tarjeta conductor	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Tarjeta conductor	personal
Driver1CurrentDailyDrivingTime	Tarjeta conductor	personal
Driver2CurrentDailyDrivingTime	Tarjeta conductor	personal
Driver1CurrentWeeklyDrivingTime	Tarjeta conductor	personal
Driver2CurrentWeeklyDrivingTime	Tarjeta conductor	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Tarjeta conductor	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Tarjeta conductor	personal
Driver1CardExpiryDate	Tarjeta conductor	personal

Datos	Fuente	Clasificación recomendada
Driver2CardExpiryDate	Tarjeta conductor	personal
Driver1CardNextMandatoryDownloadDate	Tarjeta conductor	personal
Driver2CardNextMandatoryDownloadDate	Tarjeta conductor	personal
TachographNextMandatoryDownloadDate	Unidad Vehículo	**no personal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Tarjeta conductor	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Tarjeta conductor	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Tarjeta conductor	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Tarjeta conductor	personal
Driver1CumulativeUninterruptedRestTime	Tarjeta conductor	personal
Driver2CumulativeUninterruptedRestTime	Tarjeta conductor	personal
Driver1MinimumDailyRest	Tarjeta conductor	personal
Driver2MinimumDailyRest	Tarjeta conductor	personal
Driver1MinimumWeeklyRest	Tarjeta conductor	personal
Driver2MinimumWeeklyRest	Tarjeta conductor	personal
Driver1MaximumDailyPeriod	Tarjeta conductor	personal
Driver2MaximumDailyPeriod	Tarjeta conductor	personal
Driver1MaximumDailyDrivingTime	Tarjeta conductor	personal
Driver2MaximumDailyDrivingTime	Tarjeta conductor	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Tarjeta conductor	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Tarjeta conductor	personal
Driver1RemainingCurrentDrivingTime	Tarjeta conductor	personal
Driver2RemainingCurrentDrivingTime	Tarjeta conductor	personal
GNSS position	Unidad Vehículo	personal

2) DATOS CONTINUOS DEL GNSS DISPONIBLES PREVIO CONSENTIMIENTO DEL CONDUCTOR

Véase el apéndice 12 — GNSS

3) CÓDIGOS DE INCIDENCIA DISPONIBLES SIN EL CONSENTIMIENTO DEL CONDUCTOR

Incidente	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
Inserción de una tarjeta no válida	— los 10 incidentes más recientes	— fecha y hora del incidente — tipo, número y Estado miembro emisor de la tarjeta y generación de la tarjeta que crea el incidente — número de incidentes similares ocurridos ese día
Conflicto de tarjetas	— los 10 incidentes más recientes	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente — tipo, número y Estado miembro emisor de la tarjeta y generación de las dos tarjetas que crean el conflicto
Error al cerrar la última sesión de la tarjeta	— los 10 incidentes más recientes	— fecha y hora de inserción de la tarjeta — tipo, número, Estado miembro emisor, y generación de la tarjeta — datos de la última sesión según la lectura de la tarjeta: — fecha y hora de inserción de la tarjeta — VRN, Estado miembro de matrícula y generación de la VU
Interrupción del suministro eléctrico (2)	— el incidente de más duración ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo — los 5 incidentes de mayor duración ocurridos en los últimos 365 días	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente — número de incidentes similares ocurridos ese día
Error de comunicación con la instalación de comunicación remota	— el incidente de más duración ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo — los 5 incidentes de mayor duración ocurridos en los últimos 365 días	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente — número de incidentes similares ocurridos ese día
Ausencia de información de posición del receptor del GNSS	— el incidente de más duración ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo — los 5 incidentes de mayor duración ocurridos en los últimos 365 días	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente — número de incidentes similares ocurridos ese día
Error en datos de movimiento	— el incidente de más duración ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo — los 5 incidentes de mayor duración ocurridos en los últimos 365 días	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente — número de incidentes similares ocurridos ese día

Incidente	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
Conflicto de movimiento del vehículo	— el incidente de más duración ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo — los 5 incidentes de mayor duración ocurridos en los últimos 365 días	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente — número de incidentes similares ocurridos ese día
Intento de violación de la seguridad	los 10 incidentes más recientes de cada tipo	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente (si es pertinente), — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente — tipo de incidente.
Conflicto de tiempo	— el incidente de más duración ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo — los 5 incidentes de mayor duración ocurridos en los últimos 365 días	— fecha y hora del equipo de registro — fecha y hora del GNSS — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente — número de incidentes similares ocurridos ese día

4) CÓDIGOS DE INCIDENCIA DISPONIBLES CON CONSENTIMIENTO DEL CONDUCTOR

Incidente	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
Conducción sin tarjeta adecuada	— el incidente de más duración ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo — los 5 incidentes de mayor duración ocurridos en los últimos 365 días	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente — número de incidentes similares ocurridos ese día
Inserción de tarjeta durante la conducción	— el último incidente ocurrido en cada uno de los 10 últimos días en que se hayan producido incidentes de ese tipo	— fecha y hora del incidente — tipo, número, Estado miembro emisor, y generación de la tarjeta — número de incidentes similares ocurridos ese día
Exceso de velocidad (1)	— el incidente más grave en cada uno de los 10 últimos días en que se hayan producido incidentes de este tipo (es decir, el que haya ocurrido con la velocidad media más alta) — los 5 incidentes más graves ocurridos en los últimos 365 días — el primer incidente que haya ocurrido después del último calibrado	— fecha y hora en que comenzó el incidente — fecha y hora en que terminó el incidente — velocidad máxima medida durante el incidente — media aritmética de la velocidad medida durante el incidente — tipo, número y Estado miembro emisor de la tarjeta y generación de la tarjeta del conductor (si corresponde) — número de incidentes similares ocurridos ese día

5) CÓDIGOS DE DATOS DE FALLO DISPONIBLES SIN EL CONSENTIMIENTO DEL CONDUCTOR

Fallo	Reglas de almacenamiento	Datos que hay que registrar en cada fallo
Fallo de la tarjeta	— los 10 fallos más recientes de la tarjeta del conductor	— fecha y hora en que comenzó el fallo, — fecha y hora en que terminó el fallo — tipo, número, Estado miembro emisor, y generación de la tarjeta
Fallos del aparato de control	— los 10 fallos más recientes de cada tipo — el primer fallo ocurrido después del último calibrado	— fecha y hora en que comenzó el fallo — fecha y hora en que terminó el fallo — tipo de fallo — tipo, número y Estado miembro emisor de la tarjeta, y generación de cualquier tarjeta que se haya insertado al comenzar o al terminar el incidente

Este fallo será provocado por cualquiera de los fallos siguientes, fuera del modo de calibrado:

— Fallo interno de la VU

— Fallo de la impresora

— Fallo de la pantalla

— Fallo de transferencia

— Fallo del sensor

— Fallo del receptor del GNSS o de la instalación externa del GNSS

— Fallo de la instalación de comunicación remota

6) INCIDENTES Y FALLOS ESPECÍFICOS DEL FABRICANTE SIN CONSENTIMIENTO DEL CONDUCTOR

Incidente o fallo	Reglas de almacenamiento	Datos que hay que registrar en cada incidente
A definir por el fabricante	A definir por el fabricante	A definir por el fabricante

ANEXO 2

DIAGRAMAS DE SECUENCIA DE INTERCAMBIOS DE MENSAJES CON LA UNIDAD ITS

Figura 1

Diagrama de secuencia para intento de validación con PIN

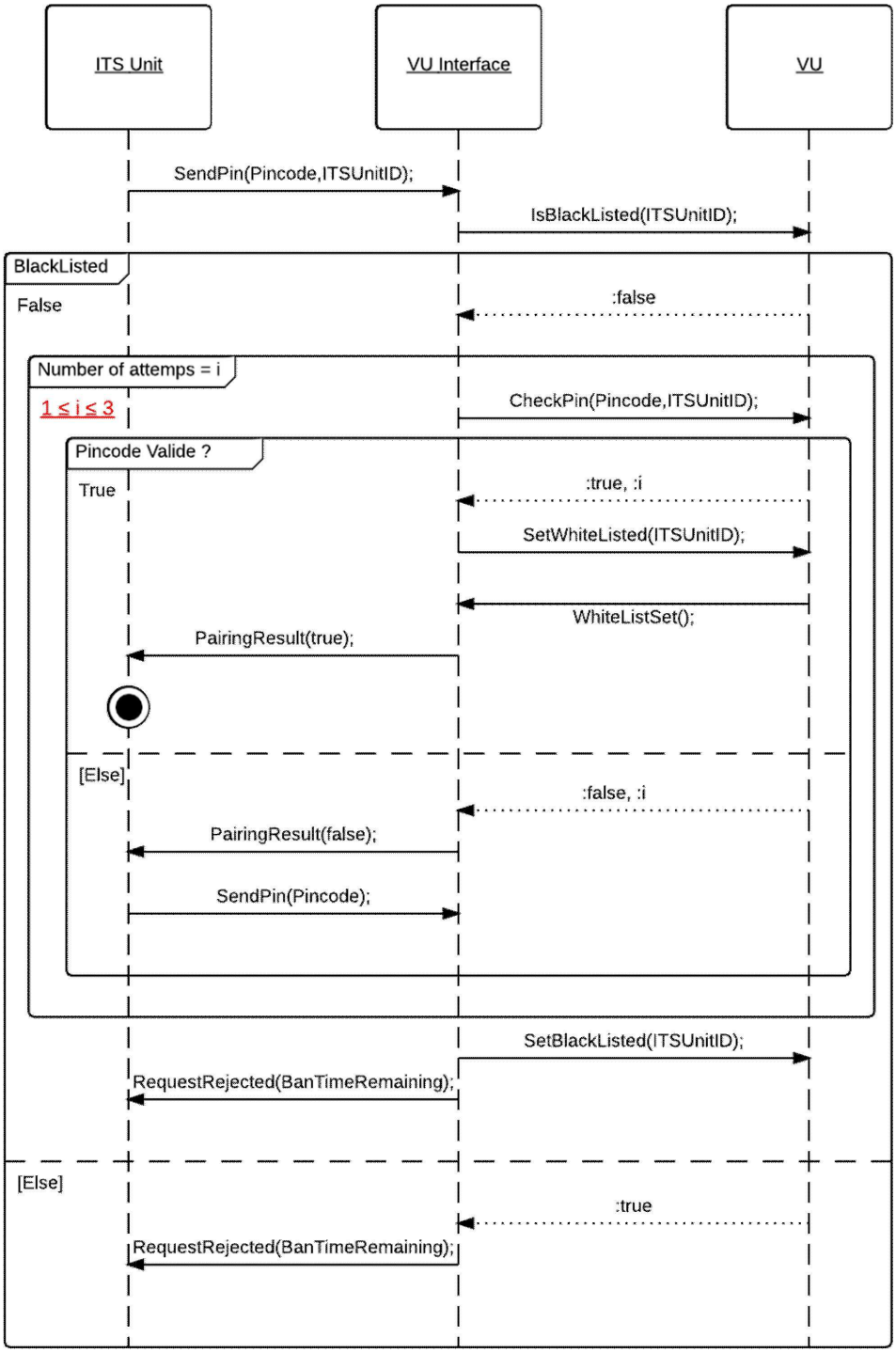


Figura 2

Diagrama de secuencia para verificación de la autorización de la unidad ITS

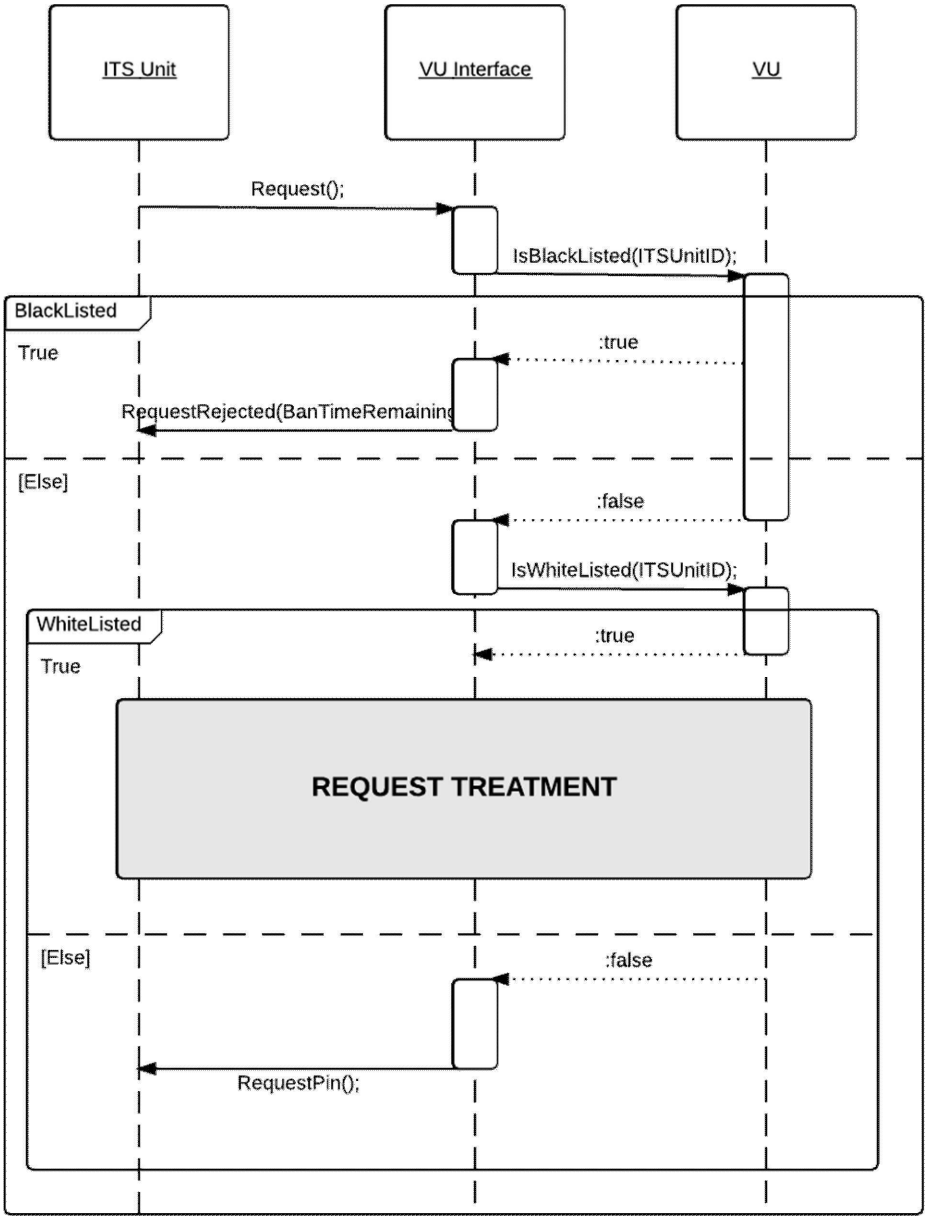


Figura 3

Diagrama de secuencia para procesar una petición de datos clasificados como no personales (previo acceso con PIN correcto)

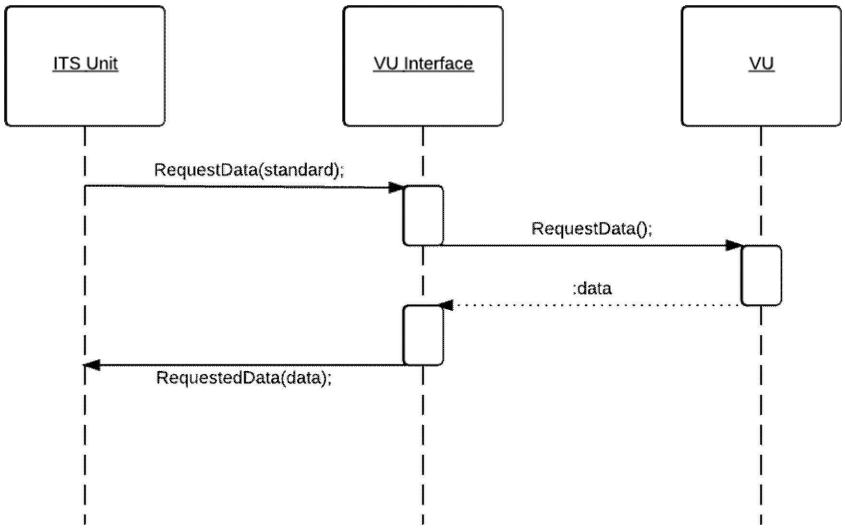


Figura 4

Diagrama de secuencia para procesar una petición de datos clasificados como personales (previo acceso con PIN correcto)

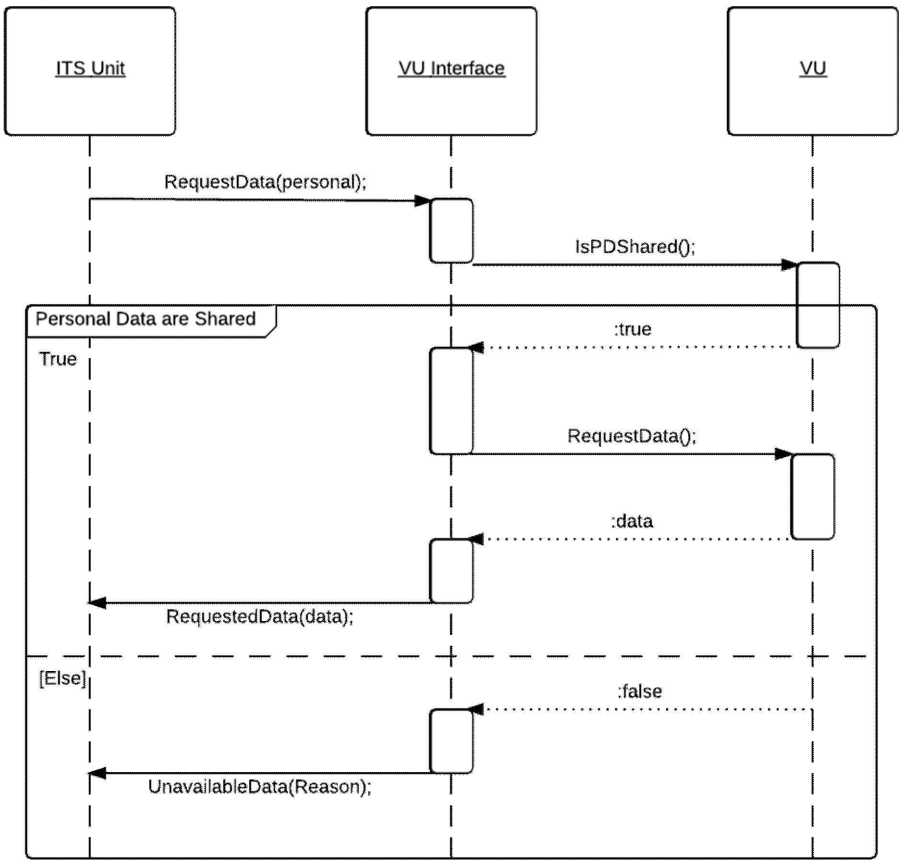
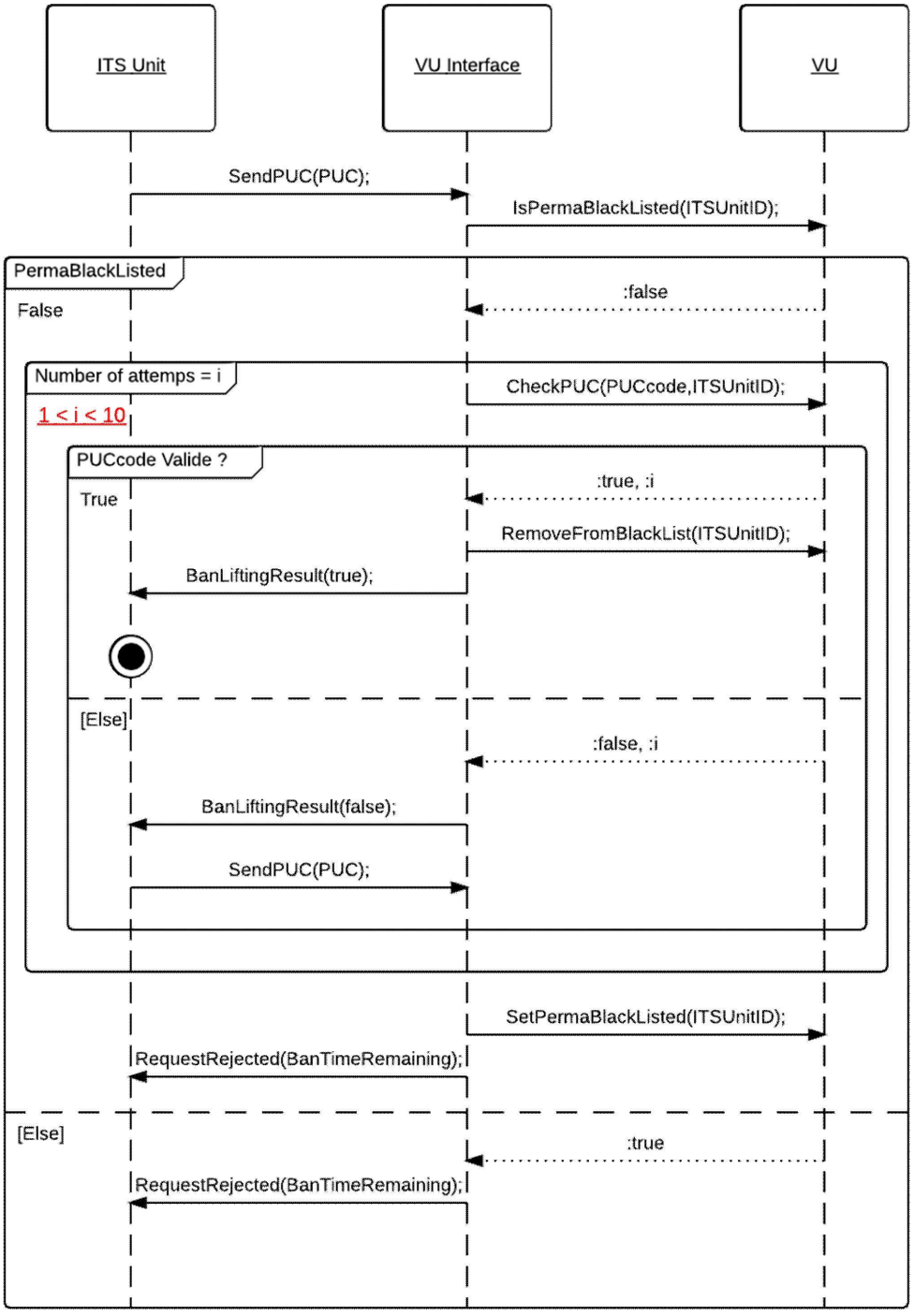


Figura 5

Diagrama de secuencia para intento de validación con PUC



ANEXO 3

ESPECIFICACIONES ASN.1

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

       CompleteMessage ::=SEQUENCE{
              header Header,
              data DataField,
              checksum Checksum
       }

       ----------------
       --HEADER TYPES--
       ----------------


       Header::=SEQUENCE{
              tgt IDList,
              src IDList,
              len BIT STRING (1..255)
       }

       vuID BIT STRING ::= 'EE'H
       IDList ::=CHOICE{
              vu BIT STRING (vuID),
              itsUnits SEQUENCE OF BIT STRING,
                     --Default hex Value:A0, redefined after first message exchange--
                     --Each ID will be linked to the Bluetooth ID of the device--
              ...
       }

       --------------------
       --DATAFIELDS TYPES--
       --------------------
       DataField ::=SEQUENCE{
              sid BIT STRING,
              trtp BIT STRING,
              subMBytes SubMessageBytes,
              dataField Content,
              ...
       }

       SubMessageBytes ::= SEQUENCE{
              currentSubM BIT STRING,
              totalSubM BIT STRING
       }

       Content ::= CHOICE{
              requestPIN RequestPIN,
              sendITSID SendITSID,
              sendPin SendPIN,
```

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

	----------
	---Utils--
	----------

	PUC ::= SEQUENCE (SIZE(8)) OF
	INTEGER (SIZE(0..9))

	PIN ::=	SEQUENCE (SIZE(4)) OF
		INTEGER (SIZE(0..9))

	--------------------------
	--Messages From ITS Unit--
	--------------------------

	SendPIN {PIN:pin} ::= SEQUENCE {
		sid BIT STRING ('03'H),
		pin PIN (pin)
	}

	SendPUC {PUC:puc} ::= SEQUENCE {
		sid BIT STRING ('05'H),
		puc PUC (puc)
	}
	--------------------
	--Messages From VU--
	--------------------

	PairingResult ::= SEQUENCE{
		sid BIT STRING ('04'H),
		result BOOLEAN
	}

	RequestPIN {MType:receivedRequest}::= SEQUENCE{
		sid BIT STRING ('01'H)
	}

	RequestRejected ::= SEQUENCE{
		sid BIT STRING ('07'H),
		banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

	BanLiftingResult ::= SEQUENCE{
		sid BIT STRING ('06'H),
		result BOOLEAN
	}
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	----------------------------
	--Complete Tachograph Data--
	----------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246           }
247
248           ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                 personal BOOLEAN (TRUE),
251                 ...
252           }
253
254           ---------------
255           --DATA SHEETS--
256           ---------------
257
258           --Data sheet format follows ISO 16844-7.--
259           StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262                 driveRecognize INTEGER (2 UNION 12),
263                 driverCardDriver1 INTEGER (2 UNION 12),
264                 driverCardDriver2 INTEGER (2 UNION 12),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267     5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270     -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                 outOfScopeCondition INTEGER(2 UNION 12),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278           vehicleRegistrationNumber SEQUENCE {
279                       codePageVRN INTEGER (0..255),
280                       vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284           }
285
286           PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                 driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289     UNION 1012...),
290                 driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291     UNION 1012...),
292
293                 driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294     1002 UNION
295                                                   1012 UNION 1102 UNION 1112 UNION
296     10002 UNION 10012 UNION
297                                                   10102 UNION 10112 UNION 11002 UNION
298     11012...),
299                 driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300     1002 UNION
```

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

             overSpeed INTEGER (2 UNION 12),
             driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver1Name DriverName,
             driver2Name DriverName,
             driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
             driver1EndOfLastDailyRestPeriod Time,
             driver2EndOfLastDailyRestPeriod Time,
             driver1EndOfLastWeeklyRestPeriod Time,
             driver2EndOfLastWeeklyRestPeriod Time,
             driver1EndOfSecondLastWeeklyRestPeriod Time,
             driver2EndOfSecondLastWeeklyRestPeriod Time,
             driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1CardExpiryDate Date,
             driver2CardExpiryDate Date,
             driver1CardNextMandatoryDownloadDate Date,
             driver2CardNextMandatoryDownloadDate Date,
             driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
             driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
             driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
537                 numberOfSimilarEvent INTEGER
538           }
539
540           PositionDataError ::= SEQUENCE{
541                 beginDate GeneralizedTime,
542                 endDate GeneralizedTime,
543                 carsdType SEQUENCE OF UTF8String,
544                 cardsNumber SEQUENCE OF INTEGER,
545                 issuingMemberState SEQUENCE OF NationAlpha,
546                 cardsGeneration SEQUENCE OF INTEGER,
547                 numberOfSimilarEvent INTEGER
548           }
549
550           MotionDataError ::= SEQUENCE{
551                 beginDate GeneralizedTime,
552                 endDate GeneralizedTime,
553                 carsdType SEQUENCE OF UTF8String,
554                 cardsNumber SEQUENCE OF INTEGER,
555                 issuingMemberState SEQUENCE OF NationAlpha,
556                 cardsGeneration SEQUENCE OF INTEGER,
557                 numberOfSimilarEvent INTEGER
558           }
559
560           VehicleMotionConflict ::= SEQUENCE{
561                 beginDate GeneralizedTime,
562                 endDate GeneralizedTime,
563                 carsdType SEQUENCE OF UTF8String,
564                 cardsNumber SEQUENCE OF INTEGER,
565                 issuingMemberState SEQUENCE OF NationAlpha,
566                 cardsGeneration SEQUENCE OF INTEGER,
567                 numberOfSimilarEvent INTEGER
568           }
569
570           SecurityBreachAttempt ::= SEQUENCE{
571                 beginDate GeneralizedTime,
572                 endDate GeneralizedTime OPTIONAL,
573                 carsdType SEQUENCE OF UTF8String,
574                 cardsNumber SEQUENCE OF INTEGER,
575                 issuingMemberState SEQUENCE OF NationAlpha,
576                 numberOfSimilarEvent INTEGER,
577                 typeOfEvent SecurityBreachEvent
578           }
579
580
581           TimeConflict ::= SEQUENCE{
582                 beginDate GeneralizedTime,
583                 endDate GeneralizedTime,
584                 carsdType SEQUENCE OF UTF8String,
585                 cardsNumber SEQUENCE OF INTEGER,
586                 issuingMemberState SEQUENCE OF NationAlpha,
587                 cardsGeneration SEQUENCE OF INTEGER,
588                 numberOfSimilarEvent INTEGER
589           }
590
591           ---------------
592           --FAULTS LIST--
593           ---------------
594
595           CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

Apéndice 14

FUNCIÓN DE COMUNICACIÓN A DISTANCIA

ÍNDICE

1 INTRODUCCIÓN

En este apéndice se especifican el diseño y los procedimientos que deben seguirse para llevar a cabo la función de comunicación a distancia (la Comunicación) con arreglo a los dispuesto en el artículo 9 del Reglamento (UE) nº 165/2014 (el Reglamento).

DSC_1 El Reglamento (UE) nº 165/2014 establece que el tacógrafo incorporará una funcionalidad de comunicación a distancia que permita que los agentes de las autoridades de control competentes puedan leer la información del tacógrafo de vehículos en circulación mediante un equipo de interrogación a distancia (el lector de teledetección temprana, REDCR), específicamente, un equipo de interrogación que se conecta de manera inalámbrica a través de interfaces de las comunicaciones especializadas de corto alcance (DSRC) de 5,8 GHz del CEN.

Es importante entender que esta funcionalidad tiene por objeto servir exclusivamente como filtro previo de selección de vehículos para controlarlos más detenidamente y no sustituye al proceso de control formal que se establece en el Reglamento (UE) nº 165/2014. Véase el considerando 9 del preámbulo de dicho Reglamento, en el que se establece que la comunicación a distancia entre el tacógrafo y las autoridades de control, con fines de control en carretera, facilita una mayor selectividad de este tipo de controles.

DSC_2 *Los Datos* se intercambiarán mediante *la Comunicación* que consistirá en un enlace inalámbrico a través de comunicaciones inalámbricas DSRC de 5,8 GHz de conformidad con el presente apéndice y evaluado con los parámetros pertinentes que se establecen en EN 300 674-1 {Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1 General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)}.

DSC_3 *La Comunicación* se establecerá con el equipo de comunicaciones solo cuando lo solicite el equipo de la autoridad de control competente por medios de radiocomunicación compatibles (*el lector de comunicación de teledetección temprana, REDCR*).

DSC_4 *Los Datos* se protegerán para garantizar su integridad.

DSC_5 El acceso a *los Datos* comunicados se restringirá a las autoridades de control competentes autorizadas para verificar las infracciones del Reglamento (CE) nº 561/2006 y del Reglamento (UE) nº 165/2014 y a los talleres en la medida en que sea necesario para verificar la funcionamiento correcto del tacógrafo.

DSC_6 El intercambio de *los Datos* durante *la Comunicación* se limitará a aquellos necesarios para hacer más selectivos los controles de carretera de los vehículos cuyo tacógrafo haya podido ser manipulado o utilizado indebidamente.

DSC_7 La integridad y la seguridad de los datos se obtendrá protegiendo *los Datos* dentro de la unidad instalada en el vehículo (VU) y transmitiendo solo los datos útiles protegidos y los datos relativos a la seguridad (véase el apartado 5.4.4) por medio de la telecomunicación inalámbrica DSRC de 5,8 GHz, lo que implica que solo las personas autorizadas de las autoridades de control competentes cuentan con los medios para interpretar los datos transmitidos a través de *la Comunicación* y para verificar su autenticidad. Véase el Apéndice 11, «Mecanismos de seguridad comunes».

DSC_8 *Los Datos* incorporarán una indicación temporal con la fecha y hora de su última actualización.

DSC_9 El contenido de los datos de seguridad solo se dará a conocer a y quedará bajo el control exclusivo de las autoridades de control competentes y aquellos terceros con los que compartan esta información y queda fuera de las disposiciones de *la Comunicación* que es objeto del presente apéndice, a menos que *la Comunicación* prevea la transferencia de un paquete de datos de seguridad con cada paquete de datos útiles.

DSC_10 La misma arquitectura y equipo podrán emplearse para obtener otros tipos de datos (como el peso a bordo) mediante la arquitectura aquí especificada.

DSC_11 A efectos de aclaración, de conformidad con las disposiciones del Reglamento (UE) nº 165/2014 (artículo 7), los datos relativos a la identidad del conductor no se transmitirán en *la Comunicación*.

2 ALCANCE

El propósito del presente apéndice es especificar el modo en que los agentes de las autoridades de control competentes utilizan una comunicación inalámbrica DSRC de 5,8 GHz específica para obtener datos a distancia de un vehículo seleccionado (*los Datos*) que indiquen que dicho vehículo ha podido infringir el Reglamento (UE) nº 165/2014 y deba ser detenido para posteriores investigaciones.

El Reglamento (UE) nº 165/2014 exige que los datos recabados se limiten o correspondan a datos que identifiquen una posible infracción, tal como se define en el artículo 9 del Reglamento (UE) nº 165/2014.

En estas circunstancias, el tiempo de que se dispone para la comunicación es limitado porque *la Comunicación* es específica y tiene un diseño de corto alcance. Además, las autoridades de control competentes pueden aprovechar el mismo medio de comunicación utilizado en la supervisión a distancia de tacógrafos (RTM) para otras aplicaciones (como los pesos máximos y las dimensiones de vehículos pesados que se establecen en la Directiva (UE) 2015/719) y estas operaciones pueden realizarse por separado o de manera consecutiva según el criterio de las autoridades de control competentes.

El presente apéndice especifica:

— el equipo, los procedimientos y los protocolos de comunicaciones que han de utilizarse para *la Comunicación*;

— las normas y los reglamentos que debe cumplir el equipo radioeléctrico;

— la presentación de *los Datos* al equipo de *la Comunicación*;

— los procedimientos de consulta y transferencia y la secuencia de las operaciones;

— *los Datos* que deben transferirse;

— la posible interpretación de *los Datos* transferidos a través de *la Comunicación*;

— las disposiciones de los datos de seguridad relativas a *la Comunicación*;

— la disponibilidad de *los Datos* para las autoridades de control competentes;

— el modo en que el *lector de comunicación de teledetección temprana* puede solicitar distintos tipos de datos sobre la carga y la flota.

A efectos de aclaración, este apéndice no especifica:

— la explotación y la gestión de la recogida de *los Datos* en la VU (que dependerá del diseño del producto a menos que se especifique de otro modo en el Reglamento (UE) nº 165/2014);

— la forma de presentar los datos recabados al agente de las autoridades de control competentes, ni los criterios que aplicarán las autoridades de control competentes para decidir qué vehículos deben detenerse (lo que dependerá del diseño del producto a menos que se especifique de otro modo en el Reglamento (UE) nº 165/2014 o en una decisión política de las autoridades de control competentes); a efectos de aclaración: *la Comunicación* se limita a poner *los Datos* a disposición de las autoridades de control competentes para que estas puedan tomar decisiones bien fundadas;

— las disposiciones sobre seguridad de los datos (como el cifrado) relativas a *los Datos* (que se especificarán en el apéndice 11, «Mecanismos de seguridad comunes»);

— detalles de cualquier tipo de datos distintos de RTM que puedan obtenerse con la misma arquitectura y equipo;

— detalles del comportamiento y la gestión entre la VU y la DSRC-VU, o el comportamiento dentro de la DSRC-VU (al margen del suministro de *los Datos* cuando los solicite un REDCR).

3 ACRÓNIMOS, DEFINICIONES Y ANOTACIONES

Los siguientes acrónimos y definiciones son específicos del presente apéndice y se utilizan como se indica a continuación:

Antena	Un dispositivo eléctrico que convierte la energía eléctrica en ondas de radio y viceversa que se utiliza con un radiotransmisor o un radiorreceptor. Cuando está en funcionamiento, un radiotransmisor suministra una corriente eléctrica que oscila a una determinada radiofrecuencia hasta los terminales de la antena y la antena irradia la energía de la corriente en forma de ondas electromagnéticas (ondas de radio). Durante la recepción, la antena intercepta parte de la energía de una onda electromagnética para generar una pequeña tensión en sus terminales que se aplica a un receptor para amplificarlo.
Comunicación	El intercambio de información o datos entre un DSRC-REDCR y una DSRC-VU conforme a lo dispuesto en la sección 5 estableciéndose una relación maestro-esclavo para obtener los datos.
Datos	Los datos protegidos en un formato definido (véase el apartado 5.4.4) solicitados por el *DSRC-REDCR* y facilitados al *DSRC-REDCR* por la *DSRC-VU* a través de un enlace DSRC de 5,8 GHz definido en la sección 5.
Reglamento (CE) nº 165/2014	El Reglamento (UE) nº 165/2014 del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, relativo a los tacógrafos en el transporte por carretera, por el que se deroga el Reglamento (CEE) nº 3821/85 relativo al aparato de control en el sector de los transportes por carretera y se modifica el Reglamento (CE) nº 561/2006 del Parlamento Europeo y del Consejo relativo a la armonización de determinadas disposiciones en materia social en el sector de los transportes por carretera.
AID	Identificador de aplicación
BLE	Bluetooth de baja energía
BST	Tabla de servicios de la baliza

CIWD	Inserción de tarjeta durante la conducción
CRC	verificación por redundancia cíclica
DSC (n)	identificador de un requisito para un apéndice DSRC específico
DSRC	Dedicated Short Range Communication
DSRC-REDCR	DSRC — lector de comunicación de teledetección temprana.
DSRC-VU	DSRC — Unidad instalada en el vehículo. Se trata del «dispositivo de teledetección temprana» definido en el anexo 1C.
DWVC	Conducción sin tarjeta válida
EID	Identificador de elementos
LLC	Control de enlace lógico
LPDU	Unidad de datos del protocolo LLC
OWS	Sistema de pesaje de a bordo
PDU	Unidad de datos de protocolo
REDCR	Lector de comunicaciones de teledetección temprana. Se trata del «lector de comunicación de teledetección temprana» definido en el anexo 1C.
RTM	Supervisión a distancia de tacógrafos
SM-REDCR	Módulo de seguridad-lector de comunicaciones de teledetección temprana
TARV	Aplicaciones telemáticas para vehículos regulados (serie de normas ISO 15638)
VU	Unidad instalada en el vehículo
VUPM	Memoria útil de la unidad instalada en el vehículo
VUSM	Módulo de seguridad de la unidad instalada en el vehículo
VST	Tabla de servicios del vehículo
WIM	Pesaje en movimiento
WOB	Pesaje a bordo

La especificación definida en este apéndice se refiere y depende de la totalidad o de distintas partes de los reglamentos y normas siguientes. En las cláusulas del presente apéndice se especifican las normas pertinentes o las cláusulas pertinentes de las normas. En el caso de exista alguna contradicción, prevalecerán las cláusulas del presente apéndice. En el caso de que exista alguna contradicción sin aclarar por alguna especificación en el presente apéndice, prevalecerán las operaciones sujetas al ERC 70-03 (y verificadas con los parámetros adecuados de EN 300 674-1), seguido en orden de preferencia por EN 12795, EN 12253 EN 12834 y EN 13372, 6.2, 6.3, 6.4 y 7.1.

Los Reglamentos y las normas mencionados en este apéndice son:

[1] Reglamento (UE) nº 165/2014 del Parlamento Europeo y del Consejo, de 4 de febrero de 2014, relativo a los tacógrafos en el transporte por carretera, por el que se deroga el Reglamento (CEE) nº 3821/85 relativo al aparato de control en el sector de los transportes por carretera y se modifica el Reglamento (CE) nº 561/2006 del Parlamento Europeo y del Consejo relativo a la armonización de determinadas disposiciones en materia social en el sector de los transportes por carretera.

[2] Reglamento (UE) nº 561/2006 del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, relativo a la armonización de determinadas disposiciones en materia social en el sector de los transportes por carretera y por el que se modifican los Reglamentos (CEE) nº 3821/85 y (CE) nº 2135/98 del Consejo y se deroga el Reglamento (CEE) nº 3820/85 del Consejo (Texto pertinente a efectos del EEE).

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1 Compatibilidad electromagnética y temas del espectro de radio (ERM); Telemática para el tráfico y el transporte por carretera (RTTT); Equipos de transmission (500 kbit/s / 250 kbit/s) operando en la banda industrial, científica y médica (ISM) de 5,8 GHz en comunicaciones dedicadas de corto alcance (DSRC); Parte 1: Características generales y métodos de ensayo para las unidades del lado de la carretera (RSU) y unidades a bordo (OBU).

[6] EN 12253 Telemática para el tráfico y el transporte por carretera (RTTT). Comunicaciones dedicadas de corto alcance (DSRC). Capa física utilizando microondas a 5,8 GHz.

[7] EN 12795 Telemática aplicada al tráfico y al transporte por carretera. Comunicaciones dedicadas de corto alcance (DSRC). Capa de enlace de datos DSRC: Control de acceso al medio y control lógico de enlace.

[8] EN 12834 Telemática para el tráfico y el transporte por carretera (RTTT). Comunicaciones dedicadas de corto alcance (DSRC) — Capa de aplicación.

[9] EN 13372 Telemática para el tráfico y el transporte por carretera (RTTT). Comunicaciones dedicadas de corto alcance (DSRC). Perfiles para aplicaciones RTTT.

[10] ISO 14906 Sistema de telepago. Definición de la interfaz de la capa de aplicación para comunicaciones dedicadas de corto alcance.

4 ESCENARIOS OPERATIVOS

4.1 **Resumen**

El Reglamento (UE) nº 165/2014 contempla escenarios específicos y controlados en los que debe utilizarse *la Comunicación*.

Los escenarios contemplados son:

«Perfil de comunicación 1: Control en carretera utilizando un lector de teledetección temprana mediante comunicación inalámbrica de corto alcance para proceder a un control físico en carretera (maestro-:-esclavo)

Perfil de lector 1a: a través de un lector de comunicaciones de teledetección temprana apuntado manualmente o instalado provisionalmente junto a la carretera y apuntado

Perfil de lector 1b: a través de un lector de comunicaciones de teledetección temprana instalado en un vehículo y dirigido».

4.1.1 *Condiciones previas a la transferencia de datos mediante una interfaz DSRC de 5,8 GHz*

NOTA: a fin de entender el contexto de las condiciones previas, se remite al lector a la figura 14.

4.1.1.1 Datos alojados en la VU

DSC_12 La VU se ocupará de actualizar cada sesenta segundos y de mantener los datos almacenados en la VU sin intervención alguna de la función de comunicación DSRC. El medio para realizar esta operación se encuentra en el interior de la VU, especificado en el Reglamento (UE) nº 165/2014, anexo 1C, sección 3.19, «*Comunicación a distancia para controles de carretera selectivos*», y no se especifica en el presente apéndice.

4.1.1.2 Datos suministrados al equipo DSRC-VU

DSC_13 La VU se ocupará de actualizar los datos del tacógrafo DSRC (*los Datos*) siempre que los datos almacenados en la VU se actualicen en el intervalo especificado en el apartado 4.1.1.1 (DSC_12), sin la intervención de la función de comunicación DSRC.

DSC_14 Los datos de la VU servirán de base para completar y actualizar *los Datos*. El medio para realizar esta operación se especifica en el anexo 1C, sección 3.19, «*Comunicación a distancia para controles de carretera selectivos*», y, de no existir dicha especificación, dependerá del diseño del producto y no se especifica en este apéndice. En cuanto al diseño de la conexión entre el equipo DSRC-VU y la VU, consúltese la sección 5.6.

4.1.1.3 Contenido de los datos

DSC_15 El contenido y el formato de *los Datos* deberán permitir que, una vez descifrados, se estructuren y se pongan a disposición del modo y con el formato especificados en el apartado 5.4.4 del presente apéndice (Estructuras de los datos).

4.1.1.4 Presentación de los datos

DSC_16 *Los Datos*, habiéndose actualizado frecuentemente conforme a los procedimientos establecidos en el apartado 4.1.1.1, se protegerán antes de su presentación a la *DSRC-VU* y se presentarán como un valor conceptual de datos seguros, para su almacenamiento temporal en la *DSRC-VU* como versión actual de *los Datos*. Estos datos se transfieren del *VUSM* a la función *VUPM* de DSRC. El *VUSM* y la *VUPM* son funciones y no necesariamente entidades físicas. La forma de instanciación física para realizar estas funciones dependerá del diseño del producto, a menos que se especifique de otro modo en el Reglamento (UE) nº 165/2014.

4.1.1.5 Datos de seguridad

DSC_17 Los datos de seguridad (*securityData*), que comprenden los datos que necesita el *REDCR* para tener la capacidad de descifrar *los Datos*, se suministrarán del modo establecido en el apéndice 11, «Mecanismos de seguridad comunes», y se presentarán como un valor conceptual de datos, para su almacenamiento temporal en la *DSRC-VU* como versión actual de *securityData*, de la forma establecida en el apartado 5.4.4 del presente apéndice.

4.1.1.6 Datos de la VUPM disponibles para su transferencia a través de la interfaz DSRC

DSC_18 El concepto de datos que deberá estar siempre disponible en la función VUPM de DSRC para su transferencia inmediata tras ser solicitados por el *REDCR* se define en el apartado 5.4.4 para todas las especificaciones del módulo ASN.1.

Descripción general del perfil de comunicación 1

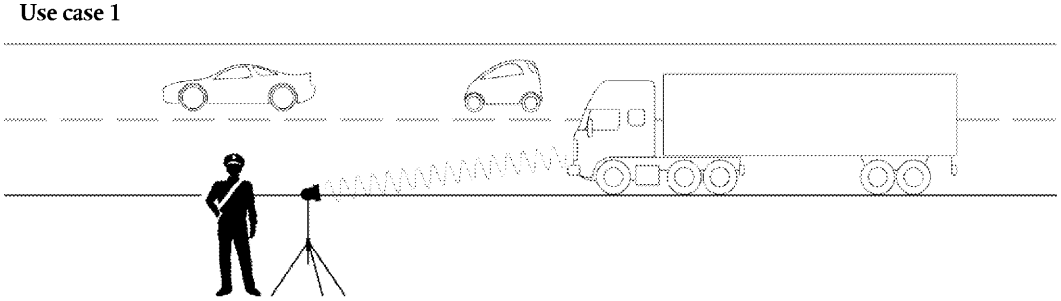
Este perfil contempla el ejemplo de uso en el que un agente de las autoridades de control competentes utiliza un lector de comunicaciones de teledetección temprana (interfaces DSRC de 5,8 GHz que operan según ERC 70-03 verificadas con los parámetros apropiados de EN 300 674-1 tal como se describe en el apartado 5) (*el REDCR*) para identificar a distancia un vehículo que pueda haber infringido el Reglamento (UE) nº 165/2014. Una vez identificado, el agente de las autoridades de control competentes que realiza la interrogación decide si debe detenerse el vehículo.

4.1.2 *Perfil 1a: mediante un lector de comunicaciones de teledetección temprana apuntado manualmente o instalado provisionalmente junto a la carretera y apuntado*

En este ejemplo de uso, el agente de las autoridades de control competentes se sitúa junto a la carretera y dirige un *REDCR* de mano, montado en un trípode o algún dispositivo portátil similar desde el lateral de la carretera hacia el centro del parabrisas del vehículo seleccionado. La interrogación se realiza mediante interfaces DSRC de 5,8 GHz que operan según ERC 70-03 y se verifican con los parámetros apropiados de EN 300 674-1 del modo descrito en el apartado 5. Véase la figura 14.1 (Ejemplo de uso 1).

Figura 14.1

Interrogación en carretera mediante DSRC de 5,8 GHz



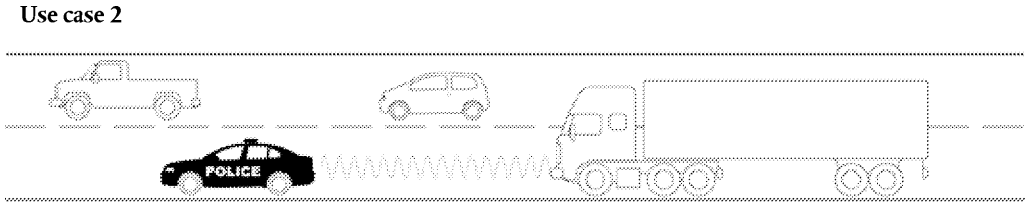
REDCR junto a la carretera

4.1.3 *Perfil 1b: mediante un lector de comunicaciones de teledetección temprana (REDCR) instalado en un vehículo y dirigido*

En este ejemplo de uso, el agente de las autoridades de control competentes se encuentra en un vehículo en movimiento y, o bien apunta un REDCR manual portátil desde el vehículo hacia el centro del parabrisas del vehículo seleccionado, o bien *el REDCR* va montado en el interior o sobre el vehículo para apuntar hacia el centro del parabrisas del vehículo seleccionado cuando el vehículo del lector de comunicaciones de teledetección temprana se encuentra en una posición determinada con relación al vehículo seleccionado (por ejemplo, directamente delante en un flujo de tráfico). La interrogación se realiza mediante interfaces DSRC de 5,8 GHz que operan según ERC 70-03 y se verifican con los parámetros apropiados de EN 300 674-1 del modo descrito en la sección 5. Véase la figura 14.2. (Ejemplo de uso 2).

Figura 14.2

Interrogación basada en vehículo mediante DSRC de 5,8 GHz (idem)



REDCR móvil

4.2 **Seguridad/Integridad**

Para poder verificar la autenticidad y la integridad de los datos transferidos a través de la comunicación a distancia, los *Datos* protegidos se verifican y se descifran según lo dispuesto en el apéndice 11, «Mecanismos de seguridad comunes».

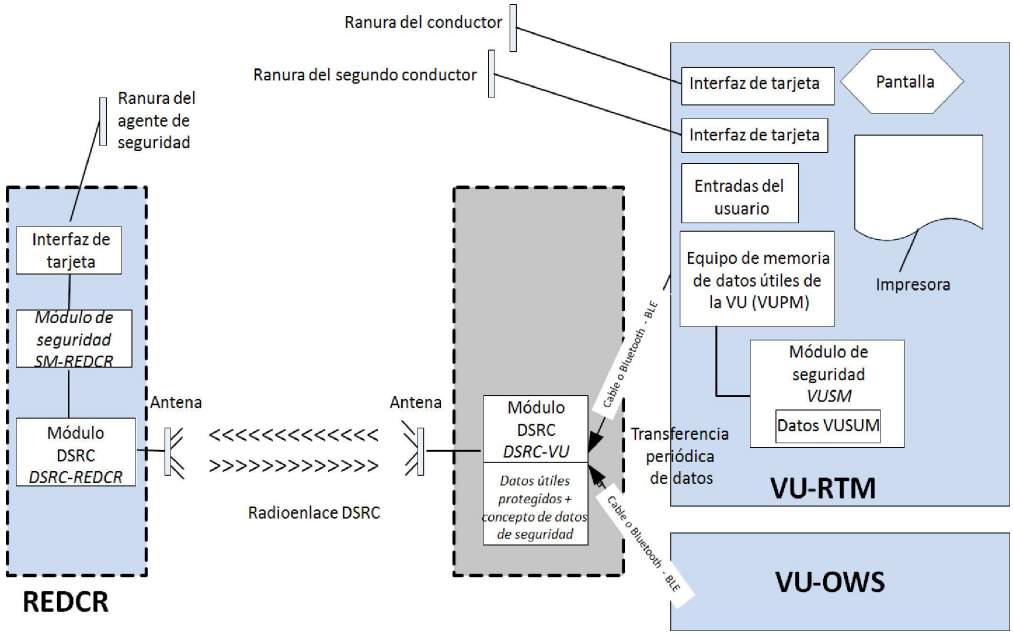
5 DISEÑO Y PROTOCOLOS DE COMUNICACIÓN A DISTANCIA

5.1 **Diseño**

El diseño de la función de comunicación a distancia del tacógrafo inteligente es el descrito en la figura 14.3.

Figura 14.3

Diseño de la función de comunicación a distancia



DSC_19 Las funciones siguientes van incorporadas a la VU:

— Módulo de seguridad (*VUSM*). Esta función incorporada a la VU se ocupa de proteger *los Datos* que se van a transmitir desde la *DSRC-VU* hasta el agente de las autoridades competentes mediante comunicación a distancia.

— Los datos protegidos se almacenan en la memoria VUSM. A los intervalos establecidos en el apartado 4.1.1.1 (DSC_12), la VU cifra y repone el concepto RTMdata (que comprende valores conceptuales de datos útiles y datos de seguridad especificados más adelante en este apéndice) alojado en la memoria de la DSRC-VU. El funcionamiento del módulo de seguridad se define en el apéndice 11, «Mecanismos de seguridad comunes», y queda fuera del ámbito del presente apéndice, su bien será necesario para realizar las actualizaciones del equipo de comunicación de la VU cada vez que cambien los datos del VUSM.

— La comunicación entre la VU y la DSRC-VU puede ser una comunicación por cable o una comunicación por Bluetooth de baja energía (BLE) y físicamente la DSRC-VU puede ir integrada con la antena en el parabrisas del vehículo, estar dentro de la VU o colocada en algún lugar intermedio.

— La DSRC-VU dispondrá de una fuente de alimentación fiable en todo momento. El modo en que se le suministra la alimentación es una cuestión de diseño.

— La memoria de la DSRC-VU no será volátil, con el fin de mantener los datos en la DSRC-VU incluso con el vehículo apagado.

— Si la comunicación entre la VU y la DSRC-VU se realiza mediante BLE y la fuente de alimentación es una batería no recargable, se sustituirá la fuente de alimentación de la DSRC-VU en cada inspección periódica y el fabricante del equipo DSRC-VU será responsable de garantizar que la alimentación sea suficiente para que dure de una inspección periódica a la siguiente, manteniendo el acceso normal a los datos mediante un REDCR durante todo el periodo sin fallos ni interrupciones.

— Equipo de «memoria útil» de VU RTM (*VUPM*). Esta función integrada en la VU se encarga de suministrar y actualizar *los Datos*. El contenido de *los Datos* («TachographPayload») se define más abajo en 5.4.4/5.4.5 y se actualiza según el intervalo establecido en el apartado 4.1.1.1 (DSC_12).

— DSRC-VU. Esta es la función, dentro de la antena o conectada a ella y en comunicación con la VU a través de una conexión por cable o inalámbrica (BLE), que aloja los datos actuales (*datos VUPM*) y gestiona la respuesta a una interrogación por medio de DSRC de 5,8 GHz. La desconexión del equipo DSRC o la interferencia con el funcionamiento del equipo DSRC durante la utilización normal del vehículo se considerarán una infracción del Reglamento (UE) nº 165/2014.

— El módulo de seguridad (REDCR) (*SM-REDCR*) constituye la función que se utiliza para descifrar y comprobar la integridad de los datos que provienen de la VU. El medio para lograr esta función se establece en el apéndice 11, «Mecanismos de seguridad comunes», y no se define en este apéndice.

— La función del equipo DSRC (REDCR) (*DSRC-REDCR*) comprende un transceptor de 5,8 GHz y el correspondiente *firmware* y *software* para gestionar *la Comunicación* con la *DSRC-VU* de conformidad con el presente apéndice.

— El *DSRC-REDCR* interroga a la *DSRC-VU* sobre el vehículo seleccionado y obtiene *los Datos* (los *datos VUPM* actuales del vehículo seleccionado) a través del enlace DSRC y procesa y almacena los datos recibidos en su *SM-REDCR*.

— La antena de la *DSRC-VU* se colocará en una posición en la que optimice la comunicación DSRC entre el vehículo y la antena del lado de la carretera (en general, en el centro o cerca del centro del parabrisas del vehículo). En vehículos ligeros, puede instalarse perfectamente en la parte superior del parabrisas.

— No habrá objetos metálicos (por ejemplo, insignias, pegatinas, bandas antirreflectantes (tintadas), parasoles, limpiaparabrisas en reposo) delante o cerca de la antena que puedan interferir en la comunicación.

— La antena se instalará de manera que su alineación óptica quede aproximadamente paralela a la superficie de la carretera.

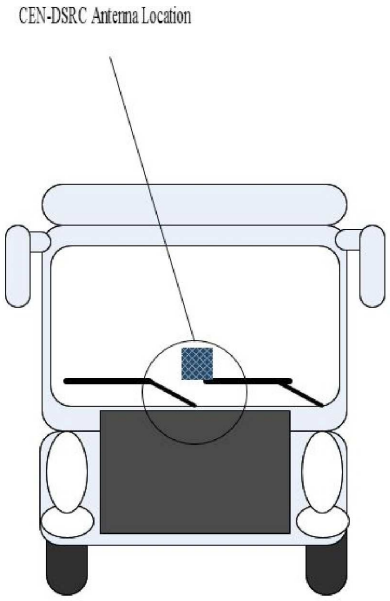
DSC_20 La Antena y la Comunicación funcionarán según ERC 70-03, verificándose con los parámetros apropiados de EN 300 674-1 del modo descrito en la sección 5. La Antena y la Comunicación pueden incorporar técnicas para atenuar el riesgo de interferencias inalámbricas según se describe en el informe ECC 228 mediante el uso, por ejemplo, de filtros en la comunicación CEN DSRC 5,8 GHz.

DSC_21 La antena DSRC se conectará al equipo DSRC-VU de forma directa dentro del módulo instalado en el parabrisas o cerca de este o mediante un cable específico fabricado de modo que dificulte su desconexión ilegal. La desconexión o interferencia con el funcionamiento de la Antena constituirá una infracción del Reglamento (UE) nº 165/2014. El enmascaramiento intencionado o perjudicial para el funcionamiento de la Antena constituirá una infracción del Reglamento (UE) nº 165/2014.

DSC_22 El factor de forma de la antena no se define y constituirá una decisión comercial, siempre que la DSRC-VU instalada cumpla los requisitos de conformidad establecidos en la sección 5. La antena se colocará del modo establecido en DSC_19 e indicado en la figura 14.4 (línea ovalada) y responderá de manera eficaz a los ejemplos de uso descritos en los apartados 4.1.2 y 4.1.3.

Figura 14.4

Ejemplo de colocación de la antena DSRC de 5,8 GHz en el parabrisas de vehículos regulados.



El factor de forma del *REDCR* y de su antena puede variar según las circunstancias del aparato de lectura (montado en un trípode, manual, instalado en un vehículo, etc.) y el *modus operandi* del agente de las autoridades del control competentes.

Se utiliza una función de visualización o notificación para mostrar los resultados de la función de comunicación a distancia al agente de las autoridades de control competentes. El modo de visualización puede ser una pantalla, una impresión en papel, una señal acústica o una combinación de las mismas. Esta forma de visualización o notificación depende de las necesidades de los agentes de las autoridades de control competentes y del diseño del equipo, por lo que no se especifica en este apéndice.

DSC_23 El diseño y el factor de forma del *REDCR* dependerá del diseño comercial, con sujeción a ERC 70-03 y a las especificaciones del diseño y rendimiento que se definen en este apéndice (apartado 5.3.2), por lo que el mercado dispone de la máxima flexibilidad para diseñar y suministrar equipos que abarquen los supuestos específicos de interrogación de cualquier autoridad de control competente.

DSC_24 El diseño y el factor de forma de la *DSRC-VU* y su posición dentro o fuera de la VU dependerán del diseño comercial, con sujeción a ERC 70-03 y a las especificaciones de diseño y rendimiento definidas en este apéndice (apartado 5.3.2) y en la presente sección (5.1).

DSC_25 No obstante, la *DSRC-VU* será razonablemente capaz de aceptar valores conceptuales de datos de otros equipos inteligentes de vehículos a través de una conexión y unos protocolos abiertos y normalizados del sector (por ejemplo, de equipos de pesaje de a bordo), siempre que estos conceptos de datos sean identificados mediante identificadores de aplicación o nombres de archivo únicos y conocidos y se faciliten a la Comisión Europea las instrucciones para manejar estos protocolos y estén disponibles sin coste para los fabricantes de los equipos pertinentes.

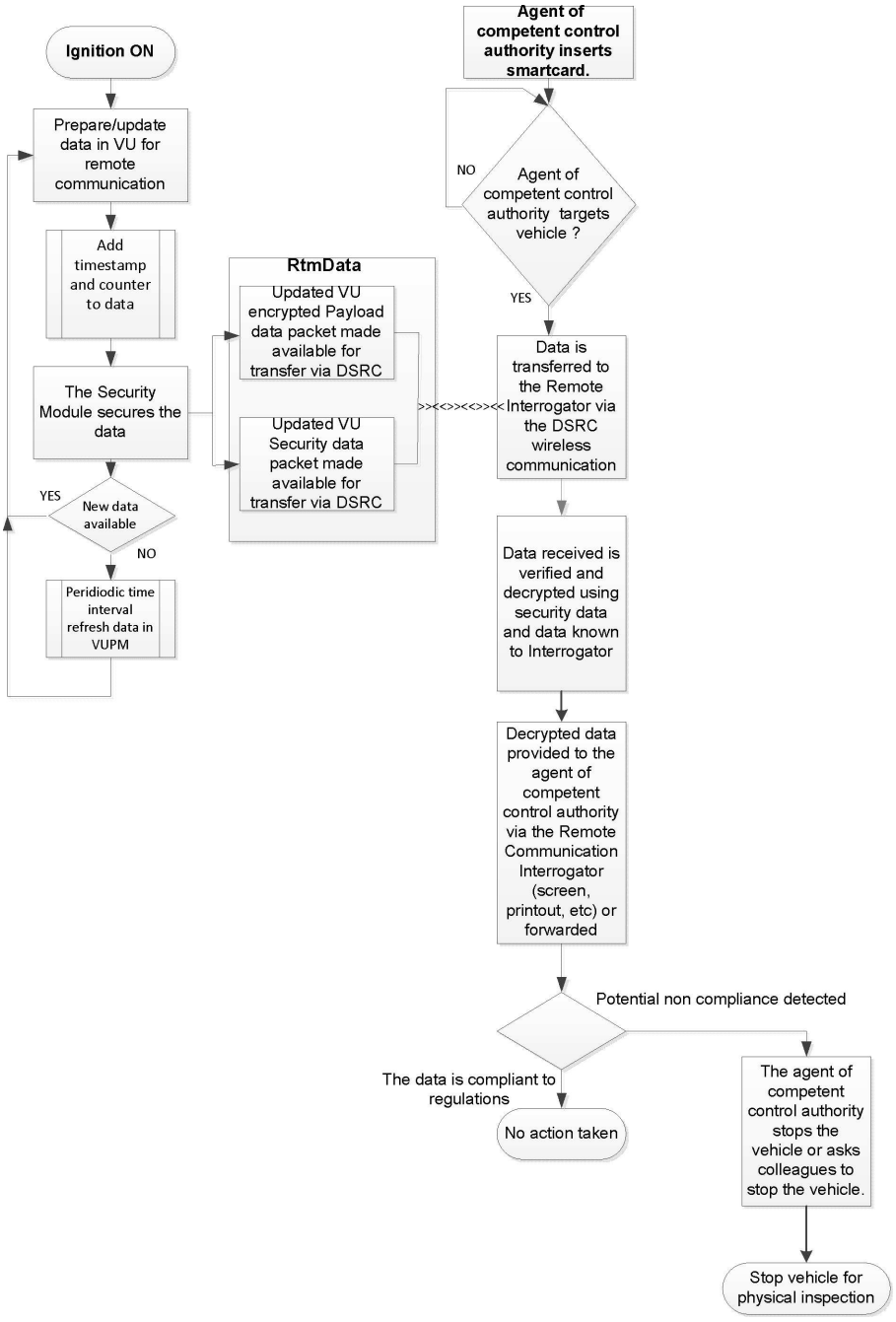
5.2 **Flujo de trabajo**

5.2.1 *Operaciones*

En la figura 14.5 se representa el flujo de trabajo de las operaciones.

Figura 14.5

Flujo de trabajo de la función de comunicación a distancia



Los pasos se describen a continuación:

a. Siempre que el vehículo esté en marcha (el encendido conectado), el tacógrafo suministra datos a la función VU. La función VU prepara *los Datos* para la función de comunicación a distancia (cifrada) y actualiza la *VUPM* y la memoria de la *DSRC-VU* (tal y como se define en los apartados 4.1.1.1 — 4.1.1.2). *Los Datos* obtenidos se formatean del modo establecido en los apartados 5.4.4 — 5.4.5.

b. Cada vez que se actualizan *los Datos*, se actualiza la indicación temporal definida en el concepto de datos de seguridad.

c. La función *VUSM* protege los datos conforme a los procedimientos establecidos en el apéndice 11.

d. Cada vez que se actualizan *los Datos* (véanse los apartados 4.1.1.1 — 4.1.1.2), *los Datos* se transfieren a la *DSRC-VU*, donde sustituyen a los datos anteriores de modo que siempre haya datos actualizados (*los Datos*) que suministrar en caso de que se produzca una interrogación por parte de un *REDCR*. Cuando la VU suministre *los Datos* al DSRC-VU, los datos podrán identificarse por el nombre del archivo *RTMData o* por los identificadores de aplicación y de atributos.

e. Si un agente de las autoridades de control competentes decide seleccionar un vehículo y recabar *los Datos* de ese vehículo específico, el agente de las autoridades de control competentes introducirá primero su tarjeta inteligente en *el REDCR* para habilitar *la Comunicación* y para que el *SM-REDCR* pueda verificar su autenticidad y descifrar los datos.

f. A continuación, el agente de las autoridades de control competentes selecciona un vehículo y solicita los datos mediante comunicación a distancia. *El REDCR* abre una sesión de interfaz de DSRC de 5,8 GHz con la *DSRC-VU* del vehículo seleccionado y solicita *los Datos*. *Los Datos* se transfieren *al REDCR* a través del sistema de comunicación inalámbrica como atributo DSRC empleando el servicio de aplicaciones GET definido en la sección 5.4. El Atributo contiene los valores de los datos útiles cifrados y los datos de seguridad de DSRC.

g. Los datos son analizados por el equipo *REDCR* y suministrados al agente de la autoridad de control competente.

h. El agente de la autoridad de control competente utiliza los datos para decidir si detiene o no el vehículo con el fin de realizar una inspección minuciosa o solicita a otro agente de la autoridad de control competente que detenga el vehículo.

5.2.2 *Interpretación de los datos recibidos a través de la comunicación DSRC*

DSC_26 Los datos recibidos a través de la interfaz de 5,8 GHz llevarán el significado y la importancia definidos en los apartados 5.4.4 y 5.4.5, y solo esos, y se entenderán únicamente en el marco de los objetivos aquí definidos. De conformidad con las disposiciones del Reglamento (UE) nº 165/2014, *los Datos* se utilizarán exclusivamente para facilitar información pertinente a una autoridad de control competente para poder determinar qué vehículo debe detener para realizar una inspección física y, posteriormente, se destruirán conforme a lo dispuesto en el artículo 9 del Reglamento (UE) nº 65/2014.

5.3 **Parámetros de la interfaz física de DSRC para comunicación a distancia**

5.3.1 *Limitaciones de posición*

DSC_27 La interrogación a distancia de vehículos mediante una interfaz DSRC de 5,8 GHz no debe utilizarse a menos de 200 metros de un pórtico DSRC de 5,8 GHz en funcionamiento.

5.3.2 *Parámetros de los enlaces ascendente y descendente*

DSC_28 El equipo empleado para la supervisión a distancia de tacógrafos se ajustará y funcionará con arreglo a ERC 70-03 y a los parámetros establecidos en los cuadros 14.1 y 14.2.

DSC_29 Asimismo, con el fin de garantizar la compatibilidad con los parámetros operativos de otros sistemas normalizados DSRC de 5,8 GHz, el equipo empleado para la supervisión a distancia de tacógrafos se ajustará a los parámetros que establecen EN 12253 y EN 13372.

A saber:

Cuadro 14.1

Parámetros de enlace descendente

Nº de elemento	Parámetro	Valor(es)	Observación
D1	Frecuencias portadoras del enlace descendente	Existen cuatro alternativas que puede utilizar un REDCR: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Dentro de ERC 70-03. El implementador puede seleccionar las frecuencias portadoras del sistema de carretera y no tienen por qué conocerse en la DSRC-VU (Conforme a EN 12253, EN 13372)
D1a (*)	Tolerancia de las frecuencias portadoras	Dentro de ± 5 ppm	(Conforme a EN 12253)
D2 (*)	Máscara del espectro del transmisor RSU (REDCR)	Dentro de ERC 70-03. El REDCR deberá ajustarse a la Clase B, C tal como se define en EN 12253 No existe ningún otro requisito específico dentro de este anexo	Parámetro utilizado para controlar las interferencias entre los interrogadores en proximidad (como se define en EN 12253 y EN 13372)
D3	Rango mínimo de frecuencias de la OBU (DSRC-VU)	5,795 — 5,815 GHz	(Conforme a EN 12253)
D4 (*)	E.I.R.P. máxima	Dentro de ERC 70-03 (sin licencia) dentro de la normativa regional Máximo +33 dBm	(Conforme a EN 12253)
D4a	Máscara de E.I.R.P. angular	Según la especificación declarada y publicada por el diseñador del interrogador	(Conforme a EN 12253)
D5	Polarización	Circular a izquierdas	(Conforme a EN 12253)
D5a	Polarización cruzada	XPD: En la dirección de máxima radiación: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB En un área a -3 dB: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(Conforme a EN 12253)
D6 (*)	Modulación	Modulación en amplitud de dos niveles.	(Conforme a EN 12253)
D6a (*)	Índice de modulación	0,5 … 0,9	(Conforme a EN 12253)

Nº de elemento	Parámetro	Valor(es)	Observación
D6b	Patrón ocular	≥ 90 % (tiempo) / ≥ 85 % (amplitud)	
D7 (*)	Codificación de datos	FM0 El bit «1» tiene transiciones solo al comienzo y al final del intervalo de bits. El bit «0» tiene una transición adicional en mitad del intervalo de bits en comparación con el bit «1».	(Conforme a EN 12253)
D8 (*)	Velocidad binaria	500 kbit/s	(Conforme a EN 12253)
D8a	Tolerancia del reloj de bit	superior a ± 100 ppm	(Conforme a EN 12253)
D9 (*)	Tasa de error de bit (B. E.R.) para comunicación	≤ 10^{-6} cuando la potencia incidente en la OBU (DSRC-VU) está en el rango dado por [D11a a D11b]	(Conforme a EN 12253)
D10	Proceso de despertar a la OBU (DSRC-VU)	La OBU (DSRC-VU) despertará al recibir una trama con 11 o más octetos (incluido el preámbulo)	No se precisa ningún patrón de activación especial La DSRC-VU puede despartarse al recibir una trama con menos de 11 octetos (Conforme a EN 12253)
D10a	Tiempo de comienzo máximo	≤ 5 ms	(Conforme a EN 12253)
D11	Zona de comunicación	Región espacial dentro de la cual la B. E.R. alcanza el valor definido por D9a	(Conforme a EN 12253)
D11a (*)	Límite superior de potencia en la zona de comunicación	– 24 dBm	(Conforme a EN 12253)
D11b (*)	Límite inferior de potencia en la zona de comunicación	Potencia incidente: – 43 dBm (dirección de máxima radiación) – 41 dBm (dentro de – 45° ± 45° respecto del plano paralelo a la superficie de la carretera cuando la DSRC-VU se instala posteriormente en el vehículo (acimut))	(Conforme a EN 12253) Requisito ampliando para ángulos horizontales hasta ± 45°, debido a los casos de uso definidos en este anexo.
D12 (*)	Nivel de potencia de corte de la OBU (DSRC-VU)	– 60 dBm	(Conforme a EN 12253)
D13	Preámbulo	Preámbulo obligatorio	(Conforme a EN 12253)
D13a	Longitud y patrón del preámbulo	16 bits ± 1 bit de bits «1» FM0 codificados	(Conforme a EN 12253)

Nº de elemento	Parámetro	Valor(es)	Observación
D13b	Forma de onda del preámbulo	Una secuencia alternativa de niveles bajos y altos con una duración de pulso de 2 µs La tolerancia viene dada por D8a	(Conforme a EN 12253)
D13c	Bits de cola	A la RSU (REDCR) se le permite transmitir un máximo de 8 bits después del indicador de final. Para la OBU (DSRC-VU) no es necesario tener en cuenta estos bits adicionales.	(Conforme a EN 12253)

(*) Los parámetros de enlace descendente están sujetos a las pruebas de conformidad de acuerdo con la prueba de parámetros pertinente de EN 300 674-1

Cuadro 14.2

Parámetros de enlace ascendente

Nº de elemento	Parámetro	Valor(es)	Observación
U1 (*)	Frecuencias de la subportadora	La OBU (DSRC-VU) debe soportar 1,5 MHz y 2,0 MHz La RSU (REDCR) debe soportar 1,5 MHz o 2,0 MHz o ambos. U1-0: 1,5 MHz U1-1: 2,0 MHz	Selección de frecuencia subportadora (1,5 MHz o 2,0 MHz) dependiendo del perfil EN 13372 elegido.
U1a (*)	Tolerancia de las frecuencias de la suportadora	dentro de ± 0,1 %	(Conforme a EN 12253)
U1b	Uso de bandas laterales	Los mismos datos en ambas bandas	(Conforme a EN 12253)
U2 (*)	Máscara de espectro de la OBU transmisora (DSRC-VU)	Conforme a EN12253 1) Potencia fuera de la banda: véase ETSI EN 300674-1 2) Potencia en la banda: [U4a] dBm en 500 kHz 3) Emisiones en cualquier otro canal de enlace ascendente: U2(3)-1 = – 35 dBm en 500 kHz	(Conforme a EN 12253)
U4a (*)	E.I.R.P. máxima de banda lateral única (alineación óptica)	Dos opciones: U4a-0: – 14 dBm U4a-1: – 21 dBm	Según la especificación declarada y publicada por el diseñador del equipo
U4b (*)	E.I.R.P. máxima de banda lateral única (35°)	Dos opciones: — No aplicable — – 17 dBm	Según la especificación declarada y publicada por el diseñador del equipo
U5	Polarización	Circular a izquierdas	(Conforme a EN 12253)

Nº de elemento	Parámetro	Valor(es)	Observación
U5a	Polarización cruzada	XPD: En la dirección de máxima radiación: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB A -3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(Conforme a EN 12253)
U6	Modulación de la subportadora	2-PSK Datos codificados sincronizados con la subportadora: las transiciones de los datos codificados coinciden con las transiciones de la subportadora	(Conforme a EN 12253)
U6b	Ciclo de trabajo	Ciclo de trabajo: 50 % ± α, α ≤ 5 %	(Conforme a EN 12253)
U6c	Modulación de la portadora	Multiplicación de la subportadora modulada con la portadora.	(Conforme a EN 12253)
U7 (*)	Codificación de datos	NRZI (Ninguna transición al comienzo del bit «1», transición al comienzo del bit «0», ninguna transición dentro del bit)	(Conforme a EN 12253)
U8 (*)	Velocidad de bit	250 kbit/s	(Conforme a EN 12253)
U8a	Tolerancia del reloj de bit	Dentro de los ± 1 000 ppm	(Conforme a EN 12253)
U9	Tasa de error de bit (B.E.R.) por comunicaciones	$\leq 10^{-6}$	(Conforme a EN 12253)
U11	Zona de comunicaciones	La región espacial en la que se sitúa la DSRC-VU de tal forma que sus transmisiones sean recibidas por el REDCR con una B.E.R. inferior a la dada por U9a.	(Conforme a EN 12253)
U12a (*)	Ganancia de conversión (límiter inferior)	1 dB por cada banda lateral Rango del ángulo: circularmente simétrico alrededor de la dirección de máxima radiación y ± 35° y	
		dentro de – 45° — + 45° respecto del plano paralelo a la superficie de la carretera cuando la DSRC-VU se instala posteriormente en el vehículo (acimut))	Superior al rango de valores especificado para los ángulos horizontales hasta ± 45°, debido a los casos de uso definidos en este anexo.
U12b (*)	Ganancia de conversión (límite superior)	10 dB por cada banda lateral	Inferior al rango de valores especificado para cada banda lateral dentro de un cono circular alrededor de la dirección de máxima radiación del ± ángulo de apertura de 45°
U13	Preámbulo	Preámbulo obligatorio	(Conforme a EN 12253)

Nº de elemento	Parámetro	Valor(es)	Observación
U13a	Preámbulo Longitud y patrón	de 32 a 36 µs modulado solamente con la subportadora, luego 8 bits de «0» codificados NRZI	(Conforme a EN 12253)
U13b	Bits de cola	La DSRC-VU puede transmitir un máximo de 8 bits tras el indicador de final. La RSU (REDCR) no necesita tener en cuenta estos bits adicionales.	(Conforme a EN 12253)

(*) – Los parámetros de enlace ascendente están sujetos a las pruebas de conformidad de acuerdo con la prueba de parámetros pertinente de EN 300 674-1

5.3.3 *Diseño de la antena*

5.3.3.1 Antena REDCR

DSC_30 El diseño de la antena *REDCR* dependerá del diseño comercial, ajustándose a los límites establecidos en el apartado 5.3.2, que se ha adaptado para optimizar el rendimiento de lectura del *DSRC-REDCR* para el fin específico y las circunstancias de lectura en las que está previsto que funcione el *REDCR*.

5.3.3.2 Antena VU

DSC_31 El diseño de la antena *DSRC-VU* dependerá del diseño comercial, ajustándose a los límites establecidos en el apartado 5.3.2, que se ha adaptado para optimizar el rendimiento de lectura del *DSRC-REDCR* para el fin específico y las circunstancias de lectura en las que el *REDCR* está previsto que funcione.

DSC_32 La antena VU se instalará en el parabrisas delantero o cerca del parabrisas delantero del vehículo del modo especificado en la sección 5.1.

DSC_33 En un entorno de pruebas de un taller (véase la sección 6.3), una antena DSRC-VU, instalada conforme a la sección 5.1, se conectará correctamente mediante una comunicación de ensayo estándar y permitirá realizar satisfactoriamente una transacción RTM del modo definido en este apéndice, a una distancia de entre 2 y 10 metros, durante un tiempo superior al 99 % y con un promedio superior a 1 000 interrogaciones de lectura.

5.4 **Requisitos del protocolo DSRC para RTM**

5.4.1 *Resumen*

DSC_34 El protocolo de transacciones para descargar *los Datos* a través del enlace de interfaz DSRC de 5,8 GHz se ajustará a los pasos indicados a continuación. Este apartado describe un flujo de transacciones en condiciones ideales sin retransmisiones ni interrupciones de la comunicación.

NOTA La finalidad de la fase de inicialización (paso 1) es configurar la comunicación entre el *REDCR* y las DSRC-VU que hayan entrado en la zona de transacción (maestro-esclavo) DSRC de 5,8 GHz pero que aún no han establecido comunicación con el *REDCR*, y notificar los procesos de la aplicación.

— **Paso 1** Inicialización. El *REDCR* envía una trama que contiene una «tabla de servicios de la baliza» (BST) que incluye los identificadores de aplicación (AID) en la lista de servicios que admite. En la aplicación RTM, consistirá simplemente en el servicio con el valor AID = 2 (carga y flota). La *DSRC-VU* evalúa la BST recibida y responde (véase a continuación) con la lista de las aplicaciones compatibles dentro del dominio de carga y flota o no responde en caso de que ninguna sea compatible. Si el *REDCR* no ofrece AID = 2, la DSRC-VU no responderá al REDCR.

— **Paso 2** La *DSRC-VU* envía una trama que contiene la solicitud de asignación de ventana privada.

— **Paso 3** El *REDCR* envía una trama que contiene una asignación de ventana privada.

— **Paso 4** La *DSRC-VU* utiliza la ventana privada asignada para enviar una trama con la tabla de servicios del vehículo (VST). Esta VST incluye una lista de todas las instanciaciones diferentes de la aplicación que admite esta *DSRC-VU* en el marco de AID = 2. Las diferentes instanciaciones se identificarán mediante EID generadas de manera única, cada una de ellas asociada a un valor del parámetro de marca contextual de la aplicación que indica la aplicación y la norma que son compatibles.

— **Paso 5** A continuación, el *REDCR* analiza la VST que se le ofrece y, o bien finaliza la conexión (RELEASE) porque no le interesa nada de lo que ofrece la VST (es decir, está recibiendo una VST de una *DSRC-VU* que no admite la transacción RTM), o bien, si recibe una VST adecuada, inicia una instanciación de la aplicación.

— **Paso 6** Para llevar esto a cabo, el REDCR enviará una trama que contiene el comando de recuperar los datos RTM e identifica la instanciación de la aplicación RTM al especificar el identificador correspondiente a la instanciación de la aplicación RTM (tal como haya sido especificado por la DSRC-VU en la VST) y asignará una ventana privada.

— **Paso 7** La *DSRC-VU* utiliza la ventana privada recién asignada para enviar una trama que contiene el identificador direccionado correspondiente a la instanciación de la aplicación RTM tal como se suministró en la VST, seguido del atributo *RtmData* (elemento de datos útiles + elemento de seguridad).

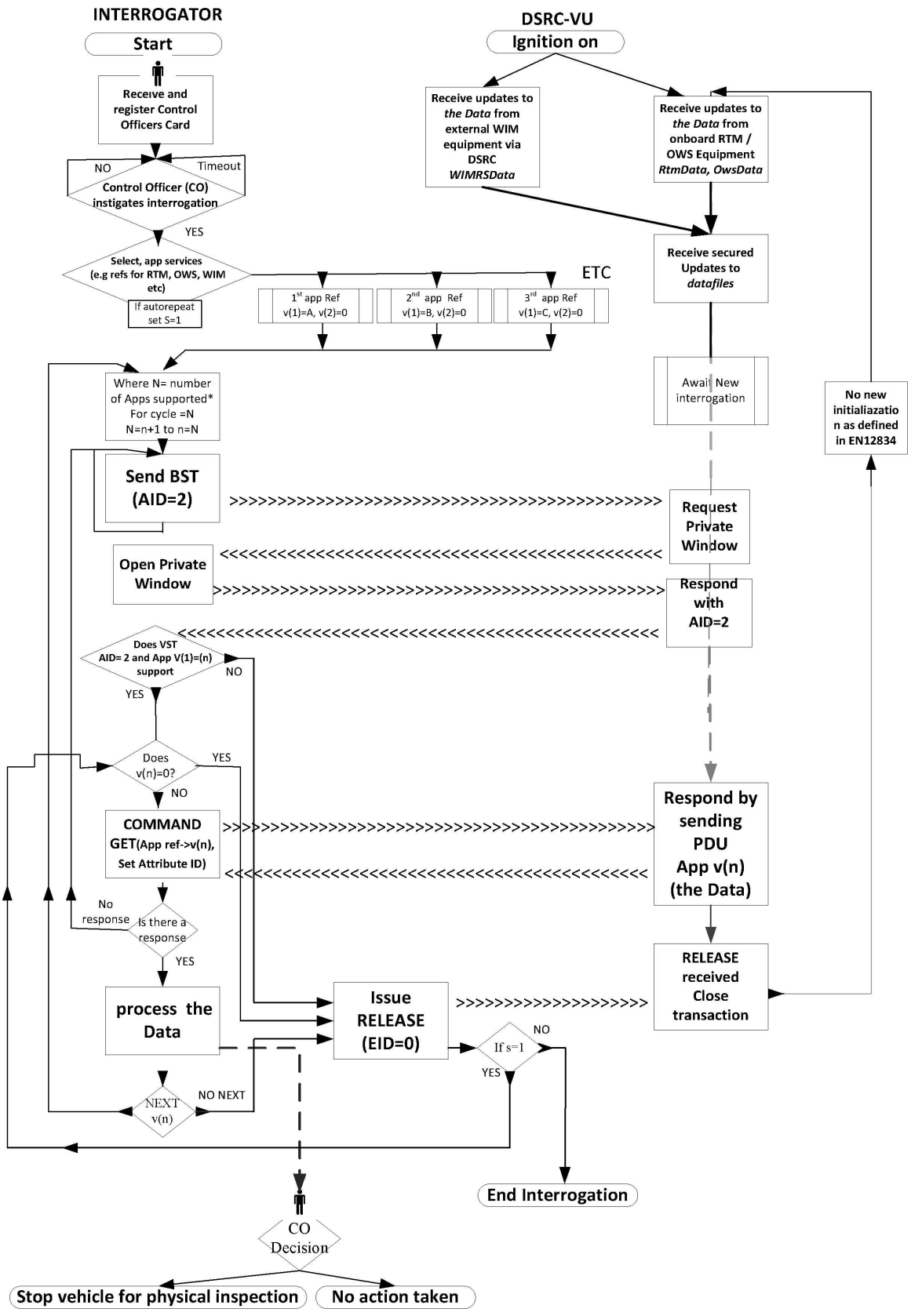
— **Paso 8** Si existen varios servicios solicitados, el valor «n» cambia al siguiente número de referencia de servicio y se repite el proceso.

— **Paso 9** El *REDCR* confirma la recepción de los datos enviando una trama que contiene el comando RELEASE a la *DSRC-VU* para finalizar la sesión O BIEN, si no consigue validar una recepción correcta de la LDPU, vuelve al paso 6.

Véase en la figura 14.6 una descripción gráfica del protocolo de transacción.

Figura 14.6

Flujo de procesos de RTM a través de una DSRC de 5,8 GHz



5.4.2 *Comandos*

DSC_35 Los siguientes comandos constituyen las únicas funciones utilizadas en una fase de transacción RTM.

— **INITIALISATION.request**: comando, enviado desde el REDCR en forma de difusión, con la definición de las aplicaciones que admite el REDCR.

— **INITIALISATION.response**: respuesta desde la DSRC-VU que confirma la conexión y contiene una lista de las instancias de aplicación admitidas con las características y la información de cómo direccionarlas (EID).

— **GET.request**: comando, enviado desde *el REDCR* a la *DSRC-VU*, que especifica la instanciación de la aplicación que debe direccionarse por medio de un EID definido, tal y como se recibió en la VST, indicando a la *DSRC-VU* que envíe los atributos seleccionados junto con *los Datos*. El objetivo del comando GET es que *el REDCR* obtenga *los Datos* de la *DSRC-VU*.

— **GET.response**: respuesta de la DSRC-VU que contiene *los Datos* solicitados.

— **ACTION.request ECHO**: comando que indica a la *DSRC-VU* que devuelva los datos desde la *DSRC-VU al REDCR*. El objetivo del comando ECHO es permitir a los talleres o centros de homologación que comprueben que el enlace DSRC funciona sin necesidad de acceder a las credenciales de seguridad.

— **ACTION**.response ECHO: respuesta desde la DSRC VU al comando ECHO.

— **EVENT_REPORT.request** RELEASE: comando que indica a la *DSRC-VU* que la transacción ha finalizado. El objetivo del comando RELEASE es finalizar la sesión con la *DSRC-VU*. Tras recibir el comando RELEASE, la *DSRC-VU* no responderá a ninguna otra interrogación durante la conexión actual. Adviértase que, según EN 12834, una DSRC-VU no se conectará dos veces con el mismo interrogador a no ser que haya estado fuera de la zona de comunicación durante 255 segundos o se cambie el ID de la baliza del interrogador.

5.4.3 *Secuencia de comandos de interrogación*

DSC_36 Desde el punto de vista de la secuencia de comandos y respuestas, la transacción se describe del modo siguiente:

Secuencia	Emisor		Receptor	Descripción	Acción
1	REDCR	>	DSRC-VU	Inicialización del enlace de comunicación — Solicitud	El REDCR difunde la BST
2	*DSRC-VU*	>	*REDCR*	*Inicialización del enlace de comunicación — Respuesta*	*Si la BST admite AID=2, entonces la DSRC-VU solicita una ventana privada*
3	REDCR	>	DSRC-VU	Concede una ventana privada	Envía una trama que contiene la asignación de la ventana privada
4	*DSRC-VU*	>	*REDCR*	*Envía una VST*	*Envía una trama que comprende una VST*
5	REDCR	>	DSRC-VU	Envía GET.request de datos en el Atributo para el EID específico	
6	*DSRC-VU*	>	*REDCR*	*Envía GET.response con el Atributo solicitado para el EID específico*	*Envía el atributo (DatosRTM, DatosOWS…) con datos para el EID específico*

Secuencia	Emisor		Receptor	Descripción	Acción
7	REDCR	>	DSRC-VU	Envía GET.request para datos de otro Atributo (si procede)	
8	*DSRC-VU*	>	*REDCR*	*Envía GET.response con el Atributo solicitado*	*Envía el Atributo con los datos para el EID específico*
9	REDCR	>	DSRC-VU	Confirma la recepción correcta de los datos	Envía el comando RELEASE, que cierra la transacción
10	*DSRC-VU*			*Cierra la transacción*	

En las cláusulas 5.4.7 y 5.4.8 se ofrece un ejemplo de la secuencia de transacción y el contenido de las tramas intercambiadas.

5.4.4 *Estructuras de los datos*

DSC_37 La estructura semántica de *los Datos* cuando pasan por la interfaz DSRC de 5,8 GHz se ajustará a lo descrito en el presente apéndice. El modo en que se estructuran estos datos se especifica en el presente apartado.

DSC_38 Los datos útiles (datos RTM) consisten en la concatenación de

1. datos EncryptedTachographPayload, que constituye el cifrado de TachographPayload definido en el apartado 5.4.5 de ASN.1. El método de cifrado se describe en el apéndice 11;

2. DSRCSecurityData, especificado en el apéndice 11.

DSC_39 Los datos RTM se están direccionando como Atributo RTM = 1 y se transfieren en el contenedor RTM = 10.

DSC_40 La marca contextual de RTM identificará la parte estándar compatible en la serie de normas TARV (RTM se corresponde con la parte 9).

La definición del módulo ASN.1 para los datos DSRC dentro de la aplicación RTM se establece del modo siguiente:

```
   TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
   DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for RTM
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


   -- Definitions of the RTM functions:
   RTM-InitialiseComm-Request ::= BST
   RTM-InitialiseComm-Response::= VST
   RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
   ABSENT,  attrIdList})
   RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})

   RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})

   RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the RTM attributes:
   RtmData ::= SEQUENCE {
        encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
   TachographPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   TachographPayload ::= SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
              tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
              tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
              tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
              tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
              tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
              tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
              tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                        -- 0= driving selected
              tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
              tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
              tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
   -- All subsequent time related types as defined in Annex 1C.
              tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
              tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
              tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
              tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
              tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
              tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
              tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
              }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]    INTEGER,
        bitstring                       [1]    BIT STRING,
        octetstring                     [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]    UniversalString,
        beaconId                        [4]    BeaconID,
        t-apdu                          [5]    T-APDUs,
        dsrcApplicationEntityId         [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]    Dsrc-EID,
        attrIdList                      [8]    AttributeIdList,
        attrList                        [9]    AttributeList{RtmContainer},
        rtmData                         [10]   RtmData,
        rtmContextmark                  [11]   Rtm-ContextMark,
        reserved12                      [12]   NULL,
        reserved13                     [13]   NULL,
        reserved14                      [14]   NULL,
        time                            [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Elementos de RtmData, acciones realizadas y definiciones*

DSC_41 Los valores de datos que debe calcular la VU y utilizar para actualizar los datos protegidos en la DSRC-VU se calcularán de acuerdo con las reglas definidas en el cuadro 14.3:

Cuadro 14.3

Elementos de RtmData, acciones realizadas y definiciones

(1) Elementos de datos RTM	(2) Acción realizada por la VU		(3) Definición de ASN.1 de los datos
RTM1 **Matrícula del vehículo**	La VU fijará el valor del elemento de datos RTM1 *tp15638VehicleRegistrationPlate* a partir del valor registrado del tipo de datos *VehicleRegistrationIdentification* tal como se define en el apéndice 1, *VehicleRegistrationIdentification*	Matrícula del vehículo expresada como una cadena de caracteres	`tp15638VehicleRegstrationPlate LPN,` `-- Matrícula del vehículo importada de ISO 14906 con la limitación especificada en EN 15509 que consiste en una SECUENCIA que comprende el código del país seguido de un indicador alfabético, seguido por el número de la matrícula propiamente dicho, que siempre tiene 14 octetos (rellenados con ceros) por lo que la longitud del tipo LPN de EN 15509 siempre es de 17 octetos, de los que 14 corresponden al número «real» de la matrícula. matrícula.`

(1) Elementos de datos RTM	(2) Acción realizada por la VU		(3) Definición de ASN.1 de los datos
RTM2 **Incidente de exceso de velocidad**	La VU generará un valor booleano para el elemento de datos RTM2 tp15638SpeedingEvent. El valor tp15638SpeedingEvent deberá ser calculado por la VU a partir del número de incidentes de exceso de velocidad registrados en la VU en los diez últimos días en que se hayan producido incidentes de este tipo, como se define en el anexo 1C. Si existe al menos un tp15638SpeedingEvent en los diez últimos días en que se hayan producido incidentes de este tipo, el valor tp15638SpeedingEvent deberá fijarse en VERDADERO. DE LO CONTRARIO, si no existen incidentes en los diez últimos días en que se hayan producido incidentes de este tipo, el valor tp15638SpeedingEvent deberá fijarse en FALSO.	1 (VERDADERO) — Indica irregularidades de velocidad en los diez últimos días en que se hayan producido incidentes de este tipo	`tp15638speedingEvent BOOLEAN,`
RTM3 **Conducir sin una tarjeta válida**	La VU generará un valor booleano para el elemento de datos RTM3 tp15638DrivingWithoutValidCard. La VU deberá asignar un valor de Verdadero a la variable tp15638DrivingWithoutValidCard si los datos de la VU registran al menos un incidente en los diez últimos días en que se hayan producido incidentes del tipo «Conducir sin una tarjeta válida» tal como se define en el anexo 1C. DE LO CONTRARIO, si no existen incidentes en los diez últimos días en que se hayan producido incidentes de este tipo, la variable tp15638DrivingWithoutValidCard se fijará en FALSO.	1 (VERDADERO) = Indica un uso de tarjeta no válido	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Tarjeta de conductor válida**	La VU generará un valor booleano para el elemento de datos RTM4 tp15638DriverCard basándose en los datos almacenados en la VU y tal como se define en el apéndice 1. Si no hay ninguna tarjeta de conductor válida, la VU deberá fijar la variable en VERDADERO. DE LO CONTRARIO, si hay una tarjeta de conductor válida, la VU deberá fijar la variable en FALSO.	0 (FALSO) = Indica una tarjeta de conductor válida	`tp15638DriverCard BOOLEAN,`
RTM5 **Inserción de tarjeta durante la conducción**	La VU generará un valor booleano para el elemento de datos RTM5. La VU deberá asignar un valor de VERDADERO a la variable tp15638CardInsertion si los datos de la VU registran en los diez últimos días en que se hayan producido incidentes al menos un incidente del tipo «Inserción de tarjeta durante la conducción» tal y como se define en el anexo 1C. DE LO CONTRARIO, si no se producen incidentes en los diez últimos días en que se hayan producido incidentes, la variable tp15638CardInsertion deberá fijarse en FALSO.	1 (VERDADERO) = Indica la inserción de tarjeta durante la conducción en los diez últimos días en que se hayan producido incidentes	`tp15638CardInsertion BOOLEAN,`
RTM6 **Error de datos de movimiento**	La VU generará un valor booleano para el elemento de datos RTM6. La VU deberá asignar un valor de VERDADERO a la variable tp15638MotionDataError si los datos de la VU registran en los diez últimos días en que se hayan producido incidentes al menos un incidente del tipo «Error de datos de movimiento» tal y como se define en el anexo 1C. DE LO CONTRARIO, si no se ha producido ningún incidente de este tipo en los diez últimos días en que se hayan producido incidentes, la variable tp15638MotionDataError deberá fijarse en FALSO.	1 (VERDADERO) = Indica error de datos de movimiento en los diez últimos días en que se hayan producido incidentes	`tp15638motionDataError BOOLEAN,`

(1) Elementos de datos RTM	(2) Acción realizada por la VU		(3) Definición de ASN.1 de los datos
RTM7 **Conflicto de movimiento del vehículo**	La VU generará un valor booleano para el elemento de datos RTM7. La VU deberá asignar un valor de VERDADERO a la variable tp15638vehicleMotionConflict si los datos de la VU registran en los diez últimos días en que se hayan producido incidentes al menos un incidente del tipo «Conflicto de movimiento del vehículo» (valor '0A'H). DE LO CONTRARIO, si no existen incidentes en los diez últimos días en que se hayan producido incidentes de este tipo, la variable tp15638vehicleMotionConflict se fijará en FALSO.	1 (VERDADERO) = Indica conflicto de movimiento en los diez últimos días en que se hayan producido incidentes	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Tarjeta del segundo conductor**	La VU generará un valor booleano para el elemento de datos RTM8 basándose en el anexo 1C («Datos de actividad del conductor» EQUIPO y SEGUNDO CONDUCTOR). Si hay una segunda tarjeta de conductor válida, la VU deberá fijar la variable en VERDADERO. DE LO CONTRARIO, si no ha una segunda tarjeta de conductor válida, la VU deberá fijar la variable en FALSO.	1 (VERDADERO) = Indica una segunda tarjeta de conductor insertada	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Actividad actual**	La VU generará un valor booleano para el elemento de datos RTM9. Si la actividad actual se registra en la VU como cualquier actividad distinta de «CONDUCCIÓN» tal y como se define en el anexo 1C, la VU deberá fijar la variable en VERDADERO. DE LO CONTRARIO, si la actividad actual se registra en la VU como «CONDUCCIÓN», la VU deberá fijar la variable en FALSO.	1 (VERDADERO) = seleccionada otra actividad; 0 (FALSO) = se ha seleccionado la conducción	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Última sesión cerrada**	La VU generará un valor booleano para el elemento de datos RTM10. Si no se cerró correctamente la última sesión de la tarjeta tal y como se define en el anexo 1C, la VU deberá fijar la variable en VERDADERO. DE LO CONTRARIO, si se cerró correctamente la última sesión de la tarjeta, la VU deberá fijar la variable en FALSO.	1 (VERDADERO) = cerrada incorrectamente 0 (FALSO) = cerrada correctamente	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Interrupción del suministro eléctrico**	La VU generará un valor entero para el elemento de datos RTM11. La VU deberá asignar un valor para la variable tp15638PowerSupplyInterruption igual a la interrupción del suministro eléctrico de mayor duración conforme al artículo 9 del Reg (UE) nº 165/2014 del tipo «Interrupción de la fuente de alimentación», tal y como se define en el anexo 1C. DE LO CONTRARIO, si en los diez últimos días en que se hayan producido incidentes no se ha producido ningún incidente de interrupción de la alimentación, el valor del entero se fijará en 0.	— Número de interrupciones de la alimentación en los diez últimos días en que se hayan producido incidentes	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

(1) Elementos de datos RTM	(2) Acción realizada por la VU		(3) Definición de ASN.1 de los datos
RTM12 **Fallo de sensor**	La VU generará un valor entero para el elemento de datos RTM12. La VU deberá asignar a la variable Sensorfault un valor de: — 1 si se ha registrado un incidente de tipo '35'H Fallo de sensor en los últimos diez días — 2 si se ha registrado un incidente de tipo Fallo del receptor GNSS (interno o externo con valores de enumeración '51'H o '52'H) en los últimos diez días — 3 si se ha registrado un incidente del tipo '53'H Fallo de comunicación del GNSS externo en los diez últimos días en que se hayan producido incidentes — 4 si se han registrado fallos tanto del sensor como del receptor GNSS en los diez últimos días en que se hayan producido incidentes — 5 si se han registrado fallos tanto del sensor como de las comunicaciones del GNSS externo en los diez últimos días en que se hayan producido incidentes — 6 si se han registrado fallos tanto del receptor GNSS como de las comunicaciones del GNSS externo en los diez últimos días en que se hayan producido incidentes — 7 si se han registrado fallos en los tres sensores en los diez últimos días en que se hayan producido incidentes. DE LO CONTRARIO, deberá asignarse un valor de 0 si no se han registrado incidentes en los diez últimos días en quese hayan producido incidentes.	— fallo del sensor un octeto según el diccionario de datos	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Ajuste de la hora**	La VU deberá general un valor entero (timeReal del apéndice 1) para el elemento de datos RTM13 basándose en la presencia de datos de Ajuste de hora tal y como se define en el anexo 1C. La VU deberá asignar el valor de la hora en que se haya producido el último incidente de datos de ajuste de hora. DE LO CONTRARIO, si no existe ningún incidente de«Ajuste de la hora», tal y como se define en el anexo 1C, en los datos de la VU, se fijará en un valor de 0.	Hora del último ajuste de la hora	`tp15638TimeAdjustment` `INTEGER(0..4294967295),`
RTM14 **Intento de violación de la seguridad**	La VU generará un valor entero (timeReal del apéndice 1) para el elemento de datos RTM14 basándose en la presencia de un incidente de intento de violación de la seguridad tal y como se define en el anexo 1C. La VU deberá fijar el valor de la hora del último incidente de intento de violación de la seguridad registrado por la VU. DE LO CONTRARIO, si en los datos de la VU no existe ningún incidente de «intento de violación de la seguridad» tal como se define en el anexo 1C, deberá fijarse un valor de 0x00FF.	Hora del último intento de violación — Valor predeterminado =0x00FF	`tp15638LatestBreachAttempt` `INTEGER(0..4294967295),`
RTM15 **Último calibrado**	La VU deberá generar un valor entero (timeReal del apéndice 1) para el elemento de datos RTM15 basándose en la presencia de datos del último calibrado tal y como se define en el anexo 1C. La VU deberá fijar el valor de la hora de los dos últimos calibrados (RTM15 y RTM16), que se fijan en VuCalibrationData definido en el apéndice 1. La VU deberá fijar el valor para RTM15 al timeReal del registro de calibrado más reciente.	Hora de los datos del último calibrado	`tp15638LastCalibrationData` `INTEGER(0..4294967295),`

(1) Elementos de datos RTM	(2) Acción realizada por la VU		(3) Definición de ASN.1 de los datos
RTM16 **Calibrado anterior**	La VU deberá generar un valor entero (timeReal del apéndice 1) para el elemento de datos RTM16 del registro de calibrado anterior al del último calibrado. DE LO CONTRARIO, si no ha habido ningún calibrado anterior, la VU deberá fijar el valor de RTM6 en 0.	Hora de los datos del calibrado anterior	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Fecha de conexión del tacógrafo**	Para el elemento de datos RTM17, la VU deberá generar un valor entero (timeReal del apéndice 1). La VU deberá fijar el valor de la hora de la instalación inicial de la VU. La VU deberá extraer estos datos de VuCalibrationData (apéndice 1) a partir de vuCalibrationRecords con CalibrationPurpose igual a: '03'H.	Fecha de conexión del tacógrafo	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Velocidad actual**	La VU generará un valor de número entero para el elemento de datos RTM18. La VU deberá fijar el valor para RTM18 en la última velocidad actual registrada en el momento de la última actualización de los RtmData.	Última velocidad actual registrada	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Indicación temporal**	Para el elemento de datos RTM19, la VU deberá generar un valor entero (timeReal del apéndice 1). La VU deberá fijar el valor para RTM19 en la hora de la última actualización de los RtmData.	Indicación temporal del registro TachographPayload actual	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Mecanismo de transferencia de datos*

DSC_42 Los datos útiles definidos anteriormente son solicitados por el REDCR tras la fase de inicialización y, a continuación, son transmitidos por la *DSRC-VU* en la ventana asignada. El REDCR utiliza el comando GET para recuperar datos.

DSC_43 En todos los intercambios DSRC, los datos se codificarán utilizando PER (Reglas de Codificación por Paquetes).

5.4.7 *Descripción detallada de la transacción DSRC*

DSC_44 La inicialización se lleva a cabo conforme a DSC_44 — DSC_48 y las cuadros 14.4 — 14.9. En la fase de inicialización, el REDCR comienza enviando una trama que contiene una BST (tabla de servicios de la baliza) según EN 12834 y EN 13372, 6.2, 6.3, 6.4 y 7.1 con los valores que se especifican a continuación en el cuadro 14.4.

Cuadro 14.4

Inicialización: valores de trama BST

Campo	Configuración
Link Identifier	Dirección de difusión
BeaconId	Según EN 12834
Time	Según EN 12834
Profile	Sin extensión, deberá usarse 0 o 1
MandApplications	Sin extensión, EID no presente, Parámetro no presente, AID=2 Carga y flota
NoMandApplications	No presente
ProfileList	Sin extensión, número de perfiles en la lista = 0
Fragmentation header	Sin fragmentación
Layer 2 settings	PDU de comandos, comando UI

En el siguiente cuadro 14.5 se recoge un ejemplo práctico de los valores especificados en el cuadro 14.4, con una indicación de las codificaciones de bits.

Cuadro 14.5

Inicialización: ejemplo del contenido de la trama BST

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Broadcast ID	1111 1111	Dirección de difusión
3	MAC Control Field	1010 0000	PDU de comandos
4	LLC Control field	0000 0011	Comando UI
5	Fragmentation header	1xxx x001	Sin fragmentación

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
6	BST	1000	Solicitud de inicialización
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Aplicaciones no obligatorias no presentes
		xxx	Identificador del fabricante
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	ID de 27 bits disponible para el fabricante
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	Hora real UNIX de 32 bits
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	Sin extensión. Perfil de ejemplo 0
17	MandApplications SEQUENCE (SIZE (0..127,...)) OF {	0000 0001	Sin extensión, número de MandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID no presente
	OPTION indicator	0	Parámetro no presente
	AID DSRCApplicationEntityID } }	00 0010	Sin extensión. AID = 2 Carga y flota

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	Sin extensión, número de perfiles en lista = 0
20	FCS	xxxx xxxx	Secuencia de control de trama
21		xxxx xxxx	
22	Flag	0111 1110	Indicador de final

DSC_45 Una *DSRC-VU*, al recibir una BST, solicita la asignación de una ventana privada, según lo especificado por EN 12795 y EN 13372, 7.1.1, sin valores RTM específicos. El cuadro 14.6 ofrece un ejemplo de codificación de bits.

Cuadro 14.6

Inicialización: contenido de la trama que solicita la asignación de una ventana privada

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Private LID	xxxx xxxx	Dirección de enlace de la DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Solicitud de ventana privada
7	FCS	xxxx xxxx	Secuencia de control de trama
8		xxxx xxxx	
9	Flag	0111 1110	Indicador de final

DSC_46 A continuación, el REDCR responde asignando una ventana privada, según lo especificado por EN 12795 y EN 13372, 7.1.1, sin valores RTM específicos.

El cuadro 14.7 ofrece un ejemplo de codificación de bits.

Cuadro 14.7

Inicialización: contenido de la trama de asignación de una ventana privada

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Private LID	xxxx xxxx	Dirección de enlace de la DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Asignación de ventana privada
7	FCS	xxxx xxxx	Secuencia de control de trama
8		xxxx xxxx	
9	Flag	0111 1110	Indicador de final

DSC_47 La *DSRC-VU*, al recibir la asignación de una ventana privada, envía su VST (tabla de servicios del vehículo) según se define en EN 12834 y EN 13372, 6.2, 6.3, 6.4 y 7.1 con los valores especificados en el cuadro 14.8, utilizando la ventana de transmisión asignada.

Cuadro 14.8

Inicialización: valores de trama VST

Campo	Configuración
Private LID	Según EN 12834
VST parameters	Relleno=0, luego para cada aplicación compatible: EID presente, parámetro presente, AID=2, EID tal como sea generado por la OBU
Parameter	Sin extensión, contiene la marca de contexto de RTM
ObeConfiguration	El campo opcional ObeStatus puede estar presente, pero no será utilizado por el REDCR
Fragmentation header	Sin fragmentación
Layer 2 settings	PDU de comandos, comando UI

DSC_48 La *DSRC-VU* deberá ser compatible con la aplicación «Carga y flota», identificada mediante el identificador de aplicación '2'. Puede que se admitan otros identificadores de aplicación, pero no aparecerán en esta VST, ya que la BST solo requiere AID = 2. El campo «Aplicaciones» contiene una lista de las instancias de aplicación admitidas en la *DSRC-VU*. Por cada instanciación de aplicación admitida, se da una referencia a la norma correspondiente, formada por una marca contextual Rtm, que se compone de un IDENTIFICADOR DE OBJETOS que representa la norma relacionada, su parte (9 para RTM) y posiblemente su versión, más un EID que genera la DSRC-VU y va asociado a esa instancia de aplicación.

En el cuadro 14.9 se recoge un ejemplo práctico de los valores especificados en el cuadro 14.8, con una indicación de las codificaciones de bits.

Cuadro 14.9

Inicialización: ejemplo del contenido de la trama VST

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Private LID	xxxx xxxx	Dirección de enlace de la DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	PDU de comandos
7	LLC Control field	0000 0011	Comando UI
8	Fragmentation header	1xxx x001	Sin fragmentación
9	VST SEQUENCE {	1001	Respuesta de inicialización
	Fill BIT STRING (SIZE(4))	0000	No usado y fijado en 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	Sin extensión. Perfil de ejemplo 0
11		0000 0001	Sin extensión, 1 aplicación
12	SEQUENCE {		
	OPTION indicator	1	EID presente
	OPTION indicator	1	Parámetro presente
	AID DSRCApplicationEntityID	00 0010	Sin extensión. AID = 2 Carga y flota
13	EID Dsrc-EID	xxxx xxxx	Definido dentro de la OBU e identifica la instancia de la aplicación.

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
14	Parameter Container {	0000 0010	Sin extensión, Opción de contenedor = 02, Cadena de octetos
15		0000 1000	Sin extensión, longitud de la marca de contexto de Rtm = 8
16	Rtm-ContextMark::= SEQUENCE {	0000 0110	Identificador de objeto de la norma admitida, parte y versión. Ejemplo: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1). El primer octeto es 06H, que es el identificador del objeto, el segundo octeto es 06H, que es su longitud. Los seis octetos siguientes codifican el identificador de objeto de ejemplo. Adviértase que solo hay presente un único elemento de la secuencia (se omite el elemento opcional RtmCom-Profile)
17	StandardIdentifier standardIdentifier	0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus no presente
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Identificador del fabricante para la DSRC-VU tal como se describe en el registro ISO 14816
27		xxxx xxxx	
28	FCS	xxxx xxxx	Secuencia de control de trama
29		xxxx xxxx	
30	Flag	0111 1110	Indicador de final

DCS_49 A continuación el REDCR lee los datos y envía un comando GET, conforme al comando GET definido en EN 13372, 6.2, 6.3, 6.4 y EN 12834, con los valores especificados en el cuadro 14.10.

Cuadro 14.10

Presentación: valores de trama de una petición GET

Campo	Configuración
Invoker Identifier (IID)	No presente
Link Identifier (LID)	Dirección de enlace de la DSRC-VU específica
Chaining	No

Campo	Configuración
Element Identifier (EID)	Según se especifica en la VST. Sin extensión
Access Credentials	No
AttributeIdList	Sin extensión, 1 atributo, AttributeID = 1 (RtmData)
Fragmentation	No
Layer2 settings	PDU de comandos, comando ACn sondeado

El cuadro 14.11 muestra un ejemplo de lectura de los datos RTM.

Cuadro 14.11

Presentación: ejemplo de trama de una petición GET

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Private LID	xxxx xxxx	Dirección de enlace de la DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU de comandos
7	LLC Control field	n111 0111	Comando ACn sondeado, bit n
8	Fragmentation header	1xxx x001	Sin fragmentación
9	Get.request SEQUENCE {	0110	Obtener solicitud
	OPTION indicator	0	Credenciales de acceso no presentes
	OPTION indicator	0	IID no presente
	OPTION indicator	1	AttributeIdList presente
	Fill BIT STRING(SIZE(1))	0	Fijar en 0
10	EID INTEGER(0..127,…)	xxxx xxxx	El EID de la instancia de la aplicación RTM, tal como se especifica en la VST. Sin extensión
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Sin extensión, número de atributos = 1
12		0000 0001	AttributeId=1, RtmData. Sin extensión

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
13	FCS	xxxx xxxx	Secuencia de control de trama
14		xxxx xxxx	
15	Flag	0111 1110	Indicador de final

DSC_50 La *DSRC-VU*, tras recibir la petición GET, envía una respuesta GET con los datos solicitados conforme a la respuesta GET definida en EN 13372, 6.2, 6.3, 6.4 y EN 12834, con los valores que se especifican en el cuadro 14.12.

Cuadro 14.12

Presentación: valores de trama de una respuesta GET

Campo	Configuración
Invoker Identifier (IID)	No presente
Link Identifier (LID)	Según EN 12834
Chaining	No
Element Identifier (EID)	Según se especifica en la VST.
Access Credentials	No
Fragmentation	No
Layer2 settings	PDU de respuesta, Respuesta disponible y comando aceptado, comando ACn

El cuadro 14.13 muestra un ejemplo de lectura de los datos RTM.

Cuadro 14.13

Presentación: ejemplo del contenido de una trama de respuesta

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Private LID	xxxx xxxx	Dirección de enlace de la DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
6	MAC Control field	1101 0000	PDU de respuesta
7	LLC Control field	n111 0111	Respuesta disponible, bit n del comando ACn
8	LLC Status field	0000 0000	Respuesta disponible y comando aceptado
9	Fragmentation header	1xxx x001	Sin fragmentación
10	Get.response SEQUENCE {	0111	Obtener respuesta
	OPTION indicator	0	IID no presente
	OPTION indicator	1	Lista de atributos presente
	OPTION indicator	0	Estado de retorno no presente
	Fill BIT STRING(SIZE(1))	0	No se utiliza
11	EID INTEGER(0..127,…)	xxxx xxxx	Respondiendo de la Instancia de aplicación RTM. Sin extensión
12	AttributeList SEQUENCE OF {	0000 0001	Sin extensión, número de atributos = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Sin extensión, AttibuteId=1 (DatosRtm)
14	AttributeValue CONTAINER {	0000 1010	Sin extensión, Opción de contenedor = 1010.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Secuencia de control de trama
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Indicador de final

DSC_51 A continuación, el REDCR cierra la conexión enviando un comando EVENT_REPORT, RELEASE conforme a EN 13372, 6.2, 6.3, 6.4 y EN 12834,7.3.8, sin valores RTM específicos. El cuadro 14.14 muestra un ejemplo de codificación de bits del comando RELEASE.

Cuadro 14.14

Finalización. Contenido de la trama EVENT_REPORT Release

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Private LID	xxxx xxxx	Dirección de enlace de la DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	La trama contiene una LPDU de comandos
7	LLC Control field	0000 0011	Comando UI
8	Fragmentation header	1xxx x001	Sin fragmentación
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Credenciales de acceso no presentes
	OPTION indicator	0	Parámetro de evento no presente
	OPTION indicator	0	IID no presente
	Mode BOOLEAN	0	No se espera respuesta
10	EID INTEGER (0..127,…)	0000 0000	Sin extensión, EID = 0 (Sistema)
11	EventType INTEGER (0..127,…) }	0000 0000	Tipo de evento 0 = Release
12	FCS	xxxx xxxx	Secuencia de control de trama
13		xxxx xxxx	
14	Flag	0111 1110	Indicador de final

DSC_52 No se espera que la *DSRC-VU* responda al comando Release. La comunicación se cierra.

5.4.8 *Descripción de la transacción de pruebas de la DSRC*

DSC_53 Deben realizarse pruebas completas que comprendan la protección de los datos tal y como se define en el apéndice 11, «Mecanismos de seguridad comunes», por personas autorizadas que tengan acceso a los procedimientos de seguridad mediante el comando GET normal definido anteriormente.

DSC_54 Las pruebas para la puesta en servicio y para las inspecciones periódicas que requieran el descifrado y la comprensión del contenido de los datos descifrados se llevarán a cabo según los especificado en el apéndice 11, «Mecanismos de seguridad comunes», y el apéndice 9, «Homologación y lista de pruebas mínimas requeridas».

No obstante, la comunicación DSRC básica puede comprobarse mediante el comando ECHO. Estas pruebas pueden exigirse para la puesta en servicio, en inspecciones periódicas o en cualquier otro momento que lo exijan la autoridad de control competente o el Reglamento (UE) nº 165/2014 (véase la sección 6).

DSC_55 Para realizar esta prueba de comunicación básica, el REDCR emite el comando ECHO durante una sesión, es decir, tras haberse completado satisfactoriamente una fase de inicialización. Por tanto, la secuencia de interacciones es similar a la de una interrogación:

— Paso 1 *El REDCR* envía una «tabla de servicios de la baliza» (BST) que incluye los identificadores de aplicación (AID) en la lista de servicios que admite. En las aplicaciones RTM, consistirá simplemente en el servicio con el valor AID = 2.

La *DSRC-VU* evalúa la BST recibida y, cuando identifica que la BST está solicitando carga y flota (AID = 2), la *DSRC-VU* responde. Si *el REDCR* no ofrece AID = 2, la *DSRC-VU* cerrará su transacción con *el REDCR*.

— Paso 2 *La DSRC-VU* envía una solicitud de una asignación de ventana privada.

— Paso 3 El REDCR envía una asignación de ventana privada.

— Paso 4 La *DSRC-VU* utiliza la ventana privada asignada para enviar su tabla de servicio del vehículo (VST). Esta VST incluye una lista de todas las instanciaciones diferentes de la aplicación que admite esta *DSRC-VU* en el marco de AID = 2. Las diferentes instanciaciones se identificarán mediante EID únicas, cada una de ellas asociada a un valor de parámetro que indica la instancia de la aplicación que es compatible.

— Paso 5 A continuación *el REDCR* analiza la VST ofrecida y, o bien finaliza la conexión (RELEASE) porque no le interesa nada de lo que ofrece la VST (es decir, está recibiendo una VST de una *DSRC-VU* que no es una RTM VU, o bien, si recibe una VST adecuada, inicia una instanciación de aplicación.

— Paso 6 El *REDCR* emitirá un comando (ECHO) a la *DSRC-VU* específica y asignará una ventana privada.

— Paso 7 La *DSRC-VU* utiliza la ventana privada recién asignada para enviar una trama de respuesta ECHO.

Los cuadros siguientes ofrecen un ejemplo práctico de una sesión de intercambio ECHO.

DSC_56 La inicialización se lleva a cabo conforme a 5.4.7 (DSC_44 — DSC_48) y los cuadros 14.4 — 14.9.

DSC_57 A continuación, el REDCR envía un comando ACTION, ECHO conforme a ISO 14906, que contiene 100 octetos de datos sin valores específicos para RTM. El cuadro 14.15 muestra el contenido de la trama que envía el REDCR.

Cuadro 14.15

ejemplo de trama de petición ACTION,ECHO

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Private LID	xxxx xxxx	Dirección de enlace de la DSRC-VU específica
3		xxxx xxxx	

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU de comandos
7	LLC Control field	n111 0111	Comando ACn sondeado, bit n
8	Fragmentation header	1xxx x001	Sin fragmentación
9	ACTION.request SEQUENCE {	0000	Solicitud de acción (ECHO)
	OPTION indicator	0	Credenciales de acceso no presentes
	OPTION indicator	1	Parámetro de acción presente
	OPTION indicator	0	IID no presente
	Mode BOOLEAN	1	Respuesta esperada
10	EID INTEGER (0..127,…)	0000 0000	Sin extensión, EID = 0 (Sistema)
11	ActionType INTEGER (0..127,…)	0000 1111	Sin extensión, solicitud de ECHO de tipo de acción
12	ActionParameter CONTAINER {	0000 0010	Sin extensión, opción de contenedor = 2
13		0110 0100	Sin extensión, longitud de cadena = 100 octetos
14		xxxx xxxx	Datos de que se debe hacer eco
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Secuencia de control de trama
115		xxxx xxxx	
116	Flag	0111 1110	Indicador de final

DSC_58 La *DSRC-VU*, al recibir la petición ECHO, envía una respuesta ECHO de 100 octetos de datos reflejando el comando recibido, según ISO 14906, sin valores específicos para RTM. El cuadro 14.16 muestra un ejemplo de codificación a nivel de bits.

Cuadro 14.16

ejemplo de trama de respuesta ACTION,ECHO

Nº octeto	Atributo/Campo	Bits en octeto	Descripción
1	FLAG	0111 1110	Indicador de comienzo
2	Private LID	xxxx xxxx	Dirección de enlace de la VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU de respuesta
7	LLC Control field	n111 0111	comando ACn, bit n
8	LLC status field	0000 0000	Respuesta disponible
9	Fragmentation header	1xxx x001	Sin fragmentación
10	ACTION.response SEQUENCE {	0001	Respuesta de acción (ECHO)
	OPTION indicator	0	IID no presente
	OPTION indicator	1	Parámetro de respuesta presente
	OPTION indicator	0	Estado de retorno no presente
	Fill BIT STRING (SIZE (1))	0	No se utiliza
11	EID INTEGER (0..127,...)	0000 0000	Sin extensión, EID = 0 (Sistema)
12	ResponseParameter CONTAINER {	0000 0010	Sin extensión, opción de contenedor = 2
13		0110 0100	Sin extensión, longitud de cadena = 100 octetos
14		xxxx xxxx	Datos de eco
...		...	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Secuencia de control de trama
115		xxxx xxxx	
116	Flag	0111 1110	Indicador de final

5.5 **Cumplimiento de la Directiva (UE) 2015/719**

5.5.1 *Resumen*

DSC_59 Con el fin de cumplir la Directiva (UE) 2015/719 relativa las dimensiones y los pesos máximos de vehículos pesados, el protocolo de transacciones para descargar los datos OWS a través de un enlace de interfaz DSRC de 5,8 GHz será el mismo que el utilizado para los datos RTM (véase el apartado 5.4.1), con la salvedad de que el identificador de objetos que se refiere a la norma TARV se ajustará a la parte 20 de la norma ISO 15638 (TARV) relativa a WOB/OWS.

5.5.2 *Comandos*

DSC_60 Los comandos empleados para una transacción OWS serán los mismos que los utilizados en una transacción RTM.

5.5.3 *Secuencia de comandos de interrogación*

DSC_61 La secuencia de comandos de interrogación para datos OWS será la misma que para los datos RTM.

5.5.4 *Estructuras de los datos*

DSC_62 Los datos útiles (datos OWS) consisten en la concatenación de

1. datos EncryptedOwsPayload, que constituyen el cifrado de OwsPayload definido en ASN.1, apartado 5.5.5. El método de cifrado será el mismo que el adoptado para los RtmData, que se especifica en el apéndice 11.

2. DSRCSecurityData, calculados con los mismos algoritmos adoptados para los RtmData, que se especifican en el apéndice 11.

5.5.5 *Módulo ASN.1 para la transacción OWS DSRC*

DSC_63. La definición del módulo ASN.1 para los datos DSRC dentro de la aplicación RTM se establece del modo siguiente:

```
TarvOws {iso(1) standard(0) 15638 part20(20)
version1(1)} DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for OWS
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

-- Definitions of the OWS functions:
OWS-InitialiseComm-Request ::= BST
OWS-InitialiseComm-Response::= VST
OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
ABSENT, iid ABSENT, attrIdList})
OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})
OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})
OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the OWS attributes:
OwsData :: = SEQUENCE {
     encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
OwsPayload as per Appendix 11 --}),
     DSRCSecurityData OCTET STRING
     }
OwsPayload :: = SEQUENCE {
           tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
           recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
goods vehicle                                                              -- with 10 Kg
resolution.
           axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
           axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                           -- with 10 Kg resolution.
           tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
     }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
     }

StandardIdentifier ::= OBJECT IDENTIFIER
  OwsContainer ::= CHOICE {
     integer                    [0]    INTEGER,
     bitstring                  [1]    BIT STRING,
     octetstring                [2]    OCTET STRING (SIZE (0..127, ...)),
     universalString            [3]    UniversalString,
     beaconId                   [4]    BeaconID,
     t-apdu                     [5]    T-APDUs,
     dsrcApplicationEntityId    [6]    DSRCApplicationEntityID,
     dsrc-Ase-Id                [7]    Dsrc-EID,
     attrIdList                 [8]    AttributeIdList,
     attrList                   [9]    AttributeList{RtmContainer},
     reserved10                 [10]   NULL,
     OwsContextmark             [11]   Ows-ContextMark,
     OwsData                    [12]   OwsData,
     reserved13                 [13]   NULL,
     reserved14                 [14]   NULL,
     time                       [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
     }}

END
```

5.5.6 *Elementos de OwsData, acciones realizadas y definiciones*

Se definen los elementos de OwsData para cumplir la Directiva (UE) 2015/719 relativa las dimensiones y los pesos máximos de vehículos pesados. Su significado es:

— recordedWeight representa el peso total medido del vehículo pesado con una resolución de 10 kg según se define en EN ISO 14906. Por ejemplo, un valor de 2 500 representa un peso de 25 toneladas.

— axlesConfiguration representa la configuración del vehículo pesado como número de ejes. La configuración se define con la máscara de 20 bits (ampliado a partir de EN ISO 14906).

Una máscara de 2 bits representa la configuración de un eje con el formato siguiente:

— el valor 00B significa que el valor «no está disponible» porque el vehículo no dispone de ningún equipo para obtener el peso sobre el eje;

— el valor 01B significa que el eje no está presente;

— el valor 10B significa que el eje está presente, que se ha calculado y obtenido el peso y aparece en el campo axlesRecordedWeight;

— el valor 11B se reserva para usos futuros.

Los 4 últimos bits se reservan para usos futuros.

Número de ejes										
Número de ejes en el tractor			Número de ejes en el remolque							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bits)

— axlesRecordedWeight representa el peso específico registrado para cada eje con una resolución de 10 kg. Se utilizan dos octetos para cada eje. Por ejemplo, un valor de 150 representa un peso de 1 500 kg.

Los demás tipos de datos se definen en el apartado 5.4.5.

5.5.7 *Mecanismos de transferencia de datos*

DSC_64 El mecanismo de transferencia de datos para datos OWS entre el interrogador y el equipo DSRC del vehículo será el mismo que para los datos RTM (véase el apartado 5.4.6).

DSC_65 La transferencia de datos entre la plataforma que obtiene los datos de pesos máximos y el equipo DSRC del vehículo se basará en la conexión física, las interfaces y el protocolo definidos en la sección 5.6.

5.6 **Transferencia de datos entre la DSRC-VU y la VU**

5.6.1 *Conexión física e interfaces*

DSC_66 La conexión entre la *VU* y la *DSRC-VU* puede realizarse por cable físico o mediante comunicación inalámbrica de corto alcance basada en Bluetooth v4.0 BLE.

DSC_67 Independientemente de la conexión física y la interfaz elegidas, deberán cumplirse los siguientes requisitos:

DSC_68 a) con el fin de poder contratar a varios proveedores el suministro de la VU y la DSRC-VU, e incluso diferentes lotes de DSRC-VU, la conexión entre la VU y la DSRC-VU será una conexión de norma abierta. La VU se conectará con la DSRC-VU:

i) mediante cable fijo de al menos 2 metros, utilizando un conector macho homologado Straight DIN 41612 H11 de 11 patillas de la DSRC-VU para conectarlo a un conector hembra homologado DIN/ISO del dispositivo VU;

ii) mediante Bluetooth de baja energía (BLE);

iii) mediante una conexión estándar ISO 11898 o SAE J1939.

DSC_69 b) la definición de las interfaces y la conexión entre la VU y la DSRC-VU debe admitir los comandos del protocolo de aplicaciones definidos en el apartado 5.6.2. y

DSC_70 c) la VU y la DSRC-VU deben ser compatibles con el funcionamiento de la transferencia de datos a través de la conexión en cuanto al rendimiento y al suministro eléctrico.

5.6.2 *Protocolo de aplicaciones*

DSC_71 El protocolo de aplicaciones entre el dispositivo de comunicación a distancia VU y la DSRC-VU tiene por objeto la transferencia periódica de datos de comunicación a distancia desde la VU al DSRC.

DSC_72 Se han identificado los siguientes comandos principales:

1. Iniciación del enlace de comunicación: petición
2. Iniciación del enlace de comunicación: respuesta
3. Envío de datos con el identificador de la aplicación RTM y los datos útiles definidos por los datos RTM.
4. Confirmación de los datos
5. Finalización del enlace de comunicación: petición
6. Finalización del enlace de comunicación: respuesta

DSC_73 En ASN1.0, los comandos anteriores pueden definirse del modo siguiente:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 La descripción de los comandos y parámetros es la siguiente:

— `RCDT-Communication Link Initialization – Request` se utiliza para inicializar el enlace de comunicación. El comando lo envía la VU a la DSRC-VU. El LinkIdentifier lo establece la VU y lo comunica a la DSRC-VU para rastrear un enlace de comunicación específico.

(*Nota:* esto sirve para admitir enlaces futuros y otras aplicaciones o módulos como el de pesaje a bordo.)

— `RCDT-Communication Link Initialization – Response` lo utiliza la DSRC-VU para responder a la petición de iniciar el enlace de comunicación. El comando lo envía la DSRC-VU a la VU. El comando da el resultado de la inicialización como respuesta = 1 (correcto) o = 0 (incorrecto).

DSC_75 La inicialización del enlace de comunicación se realizará solo tras la instalación, calibrado y arranque del motor/VU.

— `RCDT-Send Data` lo utiliza la VU para enviar los RCDTData firmados (es decir, *los Datos de comunicación a distancia*) a la DSRC-VU. Los datos se enviarán cada 60 segundos. El parámetro DataTransactionId identifica la transmisión específica de datos. El LinkIdentifier también se usa para asegurarse de que el enlace correspondiente es el correcto.

— `RCDT-Data Acknowledgment` lo envía la DSRC-VU para suministrar información a la VU acerca de la recepción de los datos de un comando RCDT–Send Data identificado mediante el parámetro DataTransactionId. El parámetro de respuesta es 1 (correcto) o = 0 (incorrecto). Si una VU recibe más de tres respuestas iguales a 0 o si `RCDT–Send Data` la VU no recibe una confirmación de datos RCDT de un comando específico RCDT-Send Data enviado anteriormente con un DataTransactionId específico, la VU generará y registrará un incidente.

— `RCDT-Communication Link Termination request` lo envía la VU a la DSRC-VU para finalizar un enlace de un LinkIdentifier específico.

DSC_76 Al reiniciar la DSRC-VU o una VU, todos los enlaces de comunicación existentes deben eliminarse, ya que podría haber enlaces «pendientes» debido a la desconexión repentina de una VU.

— `RCDT-Communication Link Termination – Response` lo envía la DSRC-VU a la VU para confirmar la petición de finalización del enlace por parte de la VU para el LinkIdentifier específico.

5.7 **Gestión de errores**

5.7.1 *Registro y comunicación de los datos en la DSRC-VU*

DSC_77 *Los Datos* deberán ser suministrados, ya protegidos, por la función *VUSM* a la *DSRC-VU*. La *VUSM* verificará que los datos registrados en la *DSRC-VU* se han grabado correctamente. El registro y la notificación de errores en la transferencia de datos de la *VU* a la memoria de la *DSRC-VU* se llevarán a cabo con el tipo EventFaultType y el valor de enumeración fijado en '62' H fallo de comunicación del *dispositivo de comunicación a distancia* junto con la indicación temporal.

DSC_78 La *VU* mantendrá un fichero identificado mediante un nombre único que resulte fácil de identificar para los inspectores con la finalidad de registrar «fallos de comunicación interna de la VU».

DSC_79 Si la VUPM intenta obtener datos de la VU desde el módulo de seguridad (para pasarlos a la DSRC-VU), pero no lo consigue, registrará el fallo con el tipo EventFaultType y el valor de enumeración fijado en '62' H fallo de comunicación del *dispositivo de comunicación a distancia* junto con la indicación temporal. El fallo de comunicación se detecta cuando no se recibe un mensaje `RCDT Data Acknowledgment` para el correspondiente `RCDT Send Data` (es decir, con el mismo DataTransactionId en los mensajes `Send Data y Acknowledgment`)durante más de tres veces consecutivas.

5.7.2 *Errores de comunicación inalámbrica*

DSC_80 La gestión de errores de comunicación deberá ajustarse a las correspondientes normas DSRC, es decir, EN 300 674-1, EN 12253, EN 12795, EN 12834 y los parámetros pertinentes de EN 13372.

5.7.2.1 *Errores de cifrado y firma*

DSC_81 Los errores de cifrado y firma se gestionarán del modo definido en el apéndice 11, «Mecanismos de seguridad comunes», y no aparecen en ninguno de los mensajes de error asociados a transferencias de datos DSRC.

5.7.2.2 *Registro de errores*

El medio DSRC consiste en una comunicación inalámbrica dinámica en un entorno de condiciones atmosféricas e interferencias inestables, especialmente en las combinaciones de «REDCR portátil» y «vehículo en movimiento» que intervienen en esta aplicación. Por tanto, es preciso establecer la diferencia entre un «fallo de lectura» y una condición de «error». En una transacción a través de una interfaz inalámbrica, los fallos de lectura son habituales y la consecuencia suele ser un reintento, es decir, retransmitir la BST y volver a intentar la secuencia, lo cual, en la mayoría de los casos, se traducirá en una conexión de comunicación satisfactoria y la transferencia de datos, a menos que el vehículo seleccionado se salga del alcance durante el tiempo necesario para retransmitir. (Es posible que una instancia «satisfactoria» de una «lectura» haya necesitado varios intentos y reintentos.)

El fallo de lectura puede deberse a que las antenas no estaban correctamente emparejadas (fallo de «apuntado»); a que una de las antenas esté apantallada (puede ser intencionado, pero también puede deberse a la presencia física de otro vehículo); a interferencias radioeléctricas, especialmente de comunicaciones WIFI de alrededor de 5,8 GHz u otras comunicaciones inalámbricas de acceso público, o puede deberse a interferencias de radares o a condiciones atmosféricas problemáticas (por ejemplo, durante una tormenta eléctrica); o sencillamente a haberse salido del alcance de la comunicación DSRC. Las instancias individuales de los fallos de lectura, por su naturaleza, no pueden registrarse simplemente porque la comunicación no tuvo lugar.

No obstante, si el agente de la autoridad de control competente selecciona un vehículo e intenta interrogar su *DSRC-VU* sin éxito en la transferencia de datos, este fallo podría deberse a una manipulación intencionada y, por tanto, el agente de la autoridad de control competente necesita un medio para registrar el fallo y alertar a otros agentes que se encuentren más adelante del lugar en el que se ha producido una infracción. Estos agentes podrán detener el vehículo y realizar una inspección física. Pero, al no haber existido ninguna comunicación, la DSRC-VU no puede suministrar datos relacionados con el fallo. Por tanto, estos informes dependerán del diseño del equipo REDCR.

Técnicamente, un «fallo de lectura» es distinto a un «error». En este contexto, un «error» es la obtención de un valor erróneo.

Los datos que se transfieren a la *DSRC-VU* ya se suministran protegidos; por tanto, deben ser verificados por el proveedor de los datos (véase la sección 5.4).

Posteriormente, se comprueban los datos transferidos a través de la interfaz aérea mediante verificación por redundancia cíclica en el nivel de las comunicaciones. Si se valida la CRC, los datos son correctos. Si no se valida la CRC, se retransmiten los datos. Estadísticamente, es tan improbable que los datos puedan pasar con éxito una CRC de forma incorrecta que esta posibilidad puede descartarse.

Si la CRC no se valida y no hay tiempo para retransmitir y recibir los datos correctos, el resultado no será un error, sino una instanciación de un tipo específico de fallo de lectura.

Los únicos datos de «fallo» significativos que pueden registrarse son los del número de iniciaciones de transacciones satisfactorias que se producen y que no se traducen en una transferencia de datos correcta al REDCR.

DSC_82 Por tanto, el *REDCR* registrará, con indicación temporal, el número de veces que se ha producido correctamente la fase de «inicialización» de una interrogación DSRC, pero se interrumpió la transacción antes de que *los Datos* fueran recuperados correctamente por el REDCR. Estos datos quedarán a disposición del agente de la autoridad de control competente y se almacenarán en la memoria del equipo REDCR. El medio empleado para esta operación dependerá del diseño del producto o de la especificación de una autoridad de control competente.

Los únicos datos de «error» significativos que pueden registrarse son el número de veces que el REDCR no logra descifrar *los Datos* recibidos. No obstante, cabe señalar que esto estará relacionado solo con la eficacia del *software* del REDCR. Los datos pueden descifrarse técnicamente y, sin embargo, no tener sentido semántico.

DSC_83 Por tanto, el *REDCR* registrará, con indicación temporal, el número de veces que ha intentado sin éxito descifrar los datos recibidos a través de la interfaz DSRC.

6 PRUEBAS PARA LA PUESTA EN SERVICIO Y LAS INSPECCIONES PERIÓDICAS DE LA FUNCIÓN DE COMUNICACIÓN A DISTANCIA

6.1 **Generalidades**

DSC_84 Se prevén dos tipos de pruebas para la función de comunicación a distancia:

1) Una prueba ECHO para validar el canal de comunicación inalámbrica *DSRC-REDCR* >>-:-<*DSRC-VU*.
2) Una prueba de seguridad de extremo a extremo para garantizar que una tarjeta de taller puede acceder al contenido de los datos cifrados y firmados que ha creado la VU y transmitidos a través del canal de comunicación inalámbrica.

6.2 **ECHO**

Esta sección contiene disposiciones elaboradas específicamente para comprobar únicamente que el enlace *DSRC-REDCR* >>-:-<*DSRC-VU* está operativo.

El objetivo del comando ECHO es permitir a los talleres o a los centros de ensayos de homologación que prueben que el enlace DSRC funciona sin necesidad de acceder a las credenciales de seguridad. Por tanto, el equipo del evaluador solo precisa poder inicializar una comunicación DSRC (enviando una BST con AID = 2) y, seguidamente, enviar un comando ECHO y, suponiendo que funcione el DSRC, recibirá una respuesta ECHO. Véanse los detalles en el apartado 5.4.8. Suponiendo que se recibe esta respuesta correctamente, es posible validar el funcionamiento correcto del enlace DSRC (*DSRC-REDCR* >>-:-<*DSRC-VU*).

6.3 **Pruebas para validar el contenido de datos seguros**

DSC_85 Esta prueba se realiza para validar de extremo a extremo el flujo de datos de seguridad. Se precisa un lector de pruebas DSRC para esta prueba. El lector de pruebas DSRC desempeña la misma función y se instala con las mismas especificaciones que el lector que utilizan los agentes de seguridad, con la salvedad de que se utiliza una tarjeta de taller en lugar de una tarjeta de control para autenticar al usuario del lector de pruebas DSRC. La prueba puede realizarse tras la activación inicial de un tacógrafo inteligente o al final del proceso de calibrado. Tras la activación, el equipo del vehículo generará y comunicará a la DSRC-VU los datos protegidos de detección temprana.

DSC_86 El personal del taller debe colocar el lector de pruebas DSRC delante del vehículo a una distancia de entre 2 y 10 metros.

DSC_87 A continuación, dicho personal insertará una tarjeta de taller en el lector de pruebas DSRC para solicitar la interrogación de los datos de detección temprana a la VU. Tras una interrogación correcta, el personal del taller accederá a los datos recibidos para asegurarse de que se ha validado su integridad y se han descifrado correctamente.

Apéndice 15

MIGRACIÓN: GESTIÓN DE LA COEXISTENCIA DE LAS GENERACIONES DE EQUIPOS

ÍNDICE

1. DEFINICIONES

A efectos del presente apéndice, se aplicarán las siguientes definiciones:

Sistema de tacógrafo inteligente: tal como se define en el presente anexo (capítulo 1: definición bbb);

Sistema de tacógrafo de primera generación: tal como se define en el presente Reglamento (artículo 2: definición 1);

Sistema de tacógrafo de segunda generación: tal como se define en el presente Reglamento (artículo 2: definición 7);

Fecha de introducción: tal como se define en el presente anexo (capítulo 1: definición ccc);

Equipo dedicado inteligente (IDE): equipo empleado para realizar la transferencia de datos, tal como se define en el apéndice 7 del presente anexo.

2. DISPOSICIONES GENERALES

2.1. Visión general de la transición

El preámbulo del presente anexo ofrece una visión general de la transición entre los sistemas de tacógrafo de la primera y de la segunda generación.

Además de las disposiciones del presente preámbulo:

— los sensores de movimiento de primera generación no serán interoperables con las unidades instaladas en el vehículo de segunda generación,

— los sensores de movimiento de segunda generación empezarán a instalarse en los vehículos al mismo tiempo que las unidades instaladas en el vehículo de segunda generación,

— la transferencia de datos y los equipos de calibrado tendrán que evolucionar con el fin de permitir el uso de las dos generaciones de aparatos de control y tarjetas de tacógrafo.

2.2. **Interoperabilidad entre la unidad instalada en el vehículo y las tarjetas**

Se entiende que los tarjetas de tacógrafo de primera generación son interoperables con las unidades instaladas en el vehículo de primera generación (de conformidad con el anexo 1B del presente Reglamento), mientras que las tarjetas de tacógrafo de segunda generación son interoperables con las unidades instaladas en el vehículo de segunda generación (de conformidad con el anexo 1C del presente Reglamento). Asimismo, serán de aplicación los siguientes requisitos:

MIG_001 Excepto en el caso indicado en los requisitos MIG_004 y MIG_005, las tarjetas de tacógrafo de primera generación podrán seguir utilizándose en las unidades instaladas en el vehículo de segunda generación hasta el final de su fecha de validez. Sus titulares, no obstante, pueden solicitar su sustitución por tarjetas de tacógrafo de segunda generación tan pronto como estén disponibles.

MIG_002 Las unidades instaladas en vehículos de segunda generación podrán utilizar cualquier tarjeta valida de primera generación insertada, ya sea de conductor, de control o de empresa.

MIG_003 Esta capacidad puede ser eliminada por el taller de forma definitiva en dichas unidades instaladas en el vehículo, de forma que las tarjetas de tacógrafo de primera generación ya no puedan aceptarse. No obstante, esto solo podrá llevarse a cabo una vez que la Comisión Europea haya puesto en marcha un procedimiento destinado a exigir a los talleres dicha actuación, por ejemplo durante cada control periódico del tacógrafo.

MIG_004 Las unidades instaladas en el vehículo de segunda generación solo podrán utilizar las tarjetas de taller de segunda generación.

MIG_005 Para determinar el modo de funcionamiento, las unidades instaladas en el vehículo de segunda generación solo podrán considerar el tipo de la tarjeta válida insertada, independientemente de su generación.

MIG_006 Cualquier tarjeta de tacógrafo válida de segunda generación deberá poder ser utilizada en unidades instaladas en el vehículo de primera generación, exactamente como una tarjeta de tacógrafo de primera generación del mismo tipo.

2.3. **Interoperabilidad entre la unidad instalada en el vehículo y los sensores de movimiento**

Se entiende que los sensores de movimiento de primera generación son interoperables con las unidades instaladas en el vehículo de primera generación, mientras que los sensores de movimiento de segunda generación son interoperables con las unidades instaladas en el vehículo de segunda generación. Asimismo, serán de aplicación los siguientes requisitos:

MIG_007 Las unidades instaladas en el vehículo de segunda generación no podrán emparejarse y utilizarse con sensores de movimiento de primera generación.

MIG_008 Los sensores de movimiento de segunda generación podrán emparejarse y utilizarse solo con unidades instaladas en el vehículo de segunda generación, o con unidades instaladas en el vehículo de las dos generaciones.

2.4. **Interoperabilidad entre las unidades instaladas en el vehículo, las tarjetas de tacógrafo y los equipos para la transferencia de datos**

MIG_009 Los equipos para la transferencia de datos podrán utilizarse con unidades instaladas en el vehículo y tarjetas de tacógrafo de una sola generación, o de las dos.

2.4.1 *Transferencia de datos directamente de la tarjeta por IDE*

MIG_010 La transferencia de los datos se realizará por IDE desde las tarjetas de tacógrafo de una generación insertadas en sus lectores de tarjetas, utilizando los mecanismos de seguridad y el protocolo de transferencia de datos de esa generación, y los datos transferidos deberán tener el formato definido para dicha generación.

MIG_011 Para permitir el control de los conductores por parte de autoridades de control no pertenecientes a la UE, también será posible la trasferencia de datos de las tarjetas de conductor (y de taller) de segunda generación exactamente de la misma manera que las tarjetas de conductor (y de taller) de primera generación. Dicha transferencia incluirá:

— EF (archivos elementales) `IC` e `ICC` no firmados,

— EF (1ª generación) `Card_Certificate` y `CA_Certificate` no firmados,

— el resto de EF con datos de aplicación (dentro del DF TACHO) requeridos por el protocolo de transferencia de datos de la tarjeta de primera generación. Esta información debe estar protegida con una firma digital, conforme a los mecanismos de seguridad de la primera generación.

Dicha trasferencia de datos no incluirá EF con datos de aplicación solo presentes en las tarjetas de conductor (y de taller) de segunda generación (EF con datos de aplicación dentro del DF TACHO_G2).

2.4.2 *Transferencia de datos de la tarjeta a través de una unidad instalada en el vehículo*

MIG_012 Los datos se trasferirán desde una tarjeta de segunda generación insertada en una unidad instalada en el vehículo de primera generación utilizando el protocolo de transferencia de datos de primera generación. La tarjeta deberá responder a los comandos de la unidad instalada en el vehículo exactamente del mismo modo que una tarjeta de primera generación y los datos transferidos deberán tener el mismo formato que los datos transferidos desde una tarjeta de primera generación.

MIG_013 Los datos se transferirán desde una tarjeta de primera generación insertada en una unidad instalada en el vehículo de segunda generación utilizando el protocolo de transferencia de datos definido en el apéndice 7 del presente anexo. La unidad instalada en el vehículo deberá enviar comandos a la tarjeta exactamente de la misma manera que una unidad instalada en el vehículo de primera generación, y los datos transferidos deberán respetar el formato definido para las tarjetas de primera generación.

2.4.3 *Transferencia de datos de la unidad instalada en el vehículo*

MIG_014 Los datos serán transferidos desde las unidades instaladas en el vehículo de segunda generación utilizando los mecanismos de seguridad de segunda generación, y el protocolo de transferencia de datos especificado en el apéndice 7 del presente anexo.

MIG_015 Para permitir el control de los conductores por parte de autoridades de control no pertenecientes a la UE y la trasferencia de los datos de la unidad instalada en el vehículo por parte de talleres no pertenecientes a la UE, también podría ser posible la opción de realizar la trasferencia de datos desde unidades instaladas en el vehículo de segunda generación utilizando los mecanismos de seguridad de la primera generación, y el protocolo de transferencia de datos de la primera generación. Los datos transferidos deberán tener el formato de los datos transferidos desde una unidad instalada en el vehículo de primera generación. Esta capacidad podrá seleccionarse mediante los comandos del menú.

2.5. **Interoperabilidad entre las unidades instaladas en el vehículo y el equipo de calibrado**

MIG_016 El equipo de calibrado podrá efectuar el calibrado de una determinada generación de tacógrafos utilizando el protocolo de calibrado de dicha generación. El equipo de calibrado se puede utilizar con tacógrafos de una sola generación, o de las dos.

3. ETAPAS PRINCIPALES DURANTE EL PERÍODO PREVIO A LA FECHA DE INTRODUCCIÓN

MIG_017 Las claves y los certificados de los ensayos estarán a disposición de los fabricantes a más tardar **treinta meses** antes de la fecha de introducción.

MIG_018 Los ensayos de interoperabilidad deberán ponerse en marcha a petición de los fabricantes a más tardar **quince meses** antes de la fecha de introducción.

MIG_019 Las claves y certificados oficiales estarán a disposición de los fabricantes a más tardar **doce meses** antes de la fecha de introducción.

MIG_020 Los Estados miembros deberán poder expedir las tarjetas de taller de segunda generación a más tardar **tres meses** antes de la fecha de introducción.

MIG_021 Los Estados miembros deberán poder expedir todos los tipos de tarjetas de tacógrafo de segunda generación a más tardar **un mes antes de la fecha de introducción**.

4. DISPOSICIONES PARA EL PERÍODO POSTERIOR A LA FECHA DE INTRODUCCIÓN

MIG_022 Tras la fecha de introducción, los Estados miembros solamente expedirán tarjetas de tacógrafo de segunda generación.

MIG_023 Los fabricantes de unidades instaladas en el vehículo y/o de sensores de movimiento estarán autorizados a producir unidades instaladas en el vehículo y sensores de movimiento de primera generación en tanto se utilicen sobre el terreno, para que los componentes que funcionen mal puedan sustituirse.

MIG_024 Los fabricantes de unidades instaladas en el vehículo y/o de sensores de movimiento estarán autorizados a solicitar y obtener el mantenimiento de la homologación de las unidades instaladas en el vehículo y sensores de movimiento de la primera generación ya homologados.

Apéndice 16

ADAPTADOR PARA VEHÍCULOS DE LAS CATEGORÍAS M 1 Y N1

ÍNDICE

1. ABREVIATURAS Y DOCUMENTOS DE REFERENCIA

1.1. **Abreviaturas**

VU Unidad instalada en el vehículo (*Vehicle Unit*)

1.2. **Normas de referencia**

ISO16844-3 Vehículos de carretera — Sistemas de tacógrafo — Parte 3: Interfaz del sensor de movimiento

2. CARACTERÍSTICAS GENERALES Y FUNCIONES DEL ADAPTADOR

2.1. **Descripción general del adaptador**

ADA_001 El adaptador proporcionará a la VU conectada unos datos de movimiento seguros representativos en todo momento de la velocidad del vehículo o de la distancia recorrida.

El adaptador está destinado únicamente a los vehículos que deben estar provistos de un aparato de control de conformidad con el presente Reglamento.

Se instalará y utilizará solo en los tipos de vehículos definidos en la letra yy) «adaptador» del anexo IC cuando no resulte posible mecánicamente instalar ningún otro tipo de sensor de movimiento existente que por su parte cumpla las disposiciones del presente anexo y sus apéndices 1 a 16.

El adaptador no estará conectado mediante una interfaz mecánica a una parte móvil del vehículo, sino a los impulsos de velocidad o distancia generados por sensores integrados o interfaces alternativas.

ADA_002 En la caja del adaptador se colocará un sensor de movimiento homologado (con arreglo a las disposiciones del presente anexo IC, sección 8, Homologación de aparatos de control y tarjetas de tacógrafo) junto con un procesador de impulsos que inducirá los impulsos de entrada al sensor de movimiento integrado. El propio sensor de movimiento integrado estará conectado a la VU, de tal modo que la interfaz entre la VU y el adaptador cumplirá los requisitos de la norma ISO16844-3.

2.2. **Funciones**

ADA_003 El adaptador ejercerá las siguientes funciones:

— interconexión y adaptación de los impulsos de velocidad de entrada,

— inducción de los impulsos de entrada al sensor de movimiento integrado,

— todas las funciones del sensor de movimiento integrado, proporcionando datos de movimiento seguros a la VU.

2.3. **Seguridad**

ADA_004 El adaptador no obtendrá la certificación de seguridad de acuerdo con el objetivo genérico de seguridad del sensor de movimiento definido en el apéndice 10 del presente anexo. En su lugar serán de aplicación los requisitos de seguridad establecidos en la sección 4.4 del presente apéndice.

3. REQUISITOS RELATIVOS AL APARATO DE CONTROL EQUIPADO CON UN ADAPTADOR

Los requisitos que figuran en los siguientes capítulos explican cómo deben entenderse los requisitos del presente anexo cuando se utiliza un adaptador. Los números de requisito correspondientes del anexo IC se indican entre paréntesis.

ADA_005 El aparato de control de todo vehículo que esté equipado con un adaptador debe cumplir todas las disposiciones del presente anexo, a menos que se especifique otra cosa en el presente apéndice.

ADA_006 Cuando se instala un adaptador, el aparato de control incluye los cables, el adaptador (incluido un sensor de movimiento) y una VU (01).

ADA_007 La función de detección de incidentes o fallos del aparato de control se modifica como sigue:

— El incidente «Interrupción del suministro eléctrico» es activado por la VU cuando el suministro eléctrico del sensor de movimiento integrado se interrumpe durante más de 200 milisegundos, fuera del modo de calibrado (79).

— El incidente «Error de datos de movimiento» es activado por la VU en caso de interrupción del flujo normal de datos entre el sensor de movimiento integrado y la VU, o en caso de producirse un error de integridad o de autenticación de datos durante el intercambio de datos entre el sensor de movimiento integrado y la VU (83).

— El incidente «Intento de violación de la seguridad» es activado por la VU ante cualquier otro incidente que afecte a la seguridad del sensor de movimiento integrado, fuera del modo de calibrado (85).

— El fallo «aparato de control» es activado por la VU ante un fallo del sensor de movimiento incorporado, fuera del modo de calibrado (88).

ADA_008 Los fallos del adaptador que podrá detectar el aparato de control serán los relativos al sensor de movimiento integrado (88).

ADA_009 La función de calibrado de la VU permitirá el emparejamiento automático del sensor de movimiento integrado con la VU (202, 204).

4. CONDICIONES DE FABRICACIÓN Y FUNCIONAMIENTO DEL ADAPTADOR

4.1. **Interconexión y adaptación de los impulsos de velocidad de entrada**

ADA_011 La interfaz de entrada del adaptador aceptará impulsos de frecuencia que representarán la velocidad del vehículo y la distancia recorrida. Las características eléctricas de los impulsos de entrada serán: *a discreción del fabricante*. Los ajustes accesibles solamente al fabricante del adaptador y al taller autorizado que efectúa la instalación del adaptador permitirán, en su caso, la interconexión correcta de la entrada del adaptador al vehículo.

ADA_012 La interfaz de la entrada del adaptador podrá, en su caso, multiplicar o dividir los impulsos de frecuencia de los impulsos de velocidad de entrada por un factor fijo, a fin de adaptar la señal a la gama de valores del factor k definida en el presente anexo (4 000 a 25 000 impulsos/km). Sólo el fabricante del adaptador y el taller autorizado que efectúa la instalación del adaptador podrán programar este factor fijo.

4.2. **Inducción de los impulsos de entrada al sensor de movimiento integrado**

ADA_013 Los impulsos de entrada, adaptados posiblemente con arreglo a lo expuesto anteriormente, serán inducidos al sensor de movimiento integrado, de modo que cada impulso de entrada será detectado por el sensor.

4.3. **Sensor de movimiento integrado**

ADA_014 El sensor de movimiento integrado será estimulado por los impulsos inducidos, lo que le permitirá generar datos de movimiento que representarán con exactitud el movimiento del vehículo, como si estuviera conectado mediante una interfaz mecánica a una parte móvil del vehículo.

ADA_015 La VU utilizará los datos de identificación del sensor de movimiento integrado para identificar el adaptador (95).

ADA_016 Se considerará que los datos de instalación almacenados en el sensor de movimiento integrado representan los datos de instalación del adaptador (122).

4.4. **Requisitos de seguridad**

ADA_017 La caja del adaptador se diseñará de manera que no pueda abrirse. Se precintará para que los intentos de manipulación física puedan detectarse con facilidad (por ejemplo, mediante inspección visual, véase ADA_035). Los precintos deberán cumplir los mismos requisitos que los precintos del sensor de movimiento (398 a 406).

ADA_018 Será imposible retirar el sensor de movimiento integrado del adaptador sin romper el precinto o precintos de la caja del adaptador o el precinto entre el sensor y la caja del adaptador (véase ADA_034).

ADA_019 El adaptador garantizará que los datos de movimiento solo se puedan procesar y extraer de la entrada del adaptador.

4.5. **Características de funcionamiento**

ADA_020 El adaptador funcionará perfectamente en el intervalo de temperaturas determinado por el fabricante.

ADA_021 El adaptador funcionará perfectamente en el intervalo higrométrico del 10 % al 90 % (214).

ADA_022 El adaptador estará protegido frente a sobretensiones, inversiones de polaridad de la fuente de alimentación y cortocircuitos (216).

ADA_023 Los adaptadores:

— reaccionarán a todo campo magnético que perturbe la detección de movimiento del vehículo; en estas circunstancias, la unidad instalada en el vehículo registrará y almacenará un fallo del sensor (88), o bien

— estarán dotados de un sensor protegido de los campos magnéticos o invulnerable a estos (217).

ADA_024 El adaptador se ajustará a la regulación internacional en el Reglamento n.º 10 de la CEPE de las Naciones Unidas, relativa a la compatibilidad electromagnética, y deberá estar protegido contra descargas electromagnéticas y fluctuaciones de la tensión (218).

4.6. **Materiales**

ADA_025 El adaptador tendrá la clase de protección (*a discreción del fabricante, dependiendo de la posición de instalación*) (220, 221).

ADA_026 La caja del adaptador será de color amarillo.

4.7. **Inscripciones**

ADA_027 El adaptador llevará una placa descriptiva con la información siguiente:

— nombre y domicilio del fabricante del adaptador,

— número de pieza del fabricante y año de fabricación del adaptador,

— marca de homologación del modelo de adaptador o del aparato de control que incluye el adaptador,

— fecha de instalación del adaptador,

— VIN del vehículo en el que se ha instalado.

ADA_028 Además, la placa descriptiva deberá contener la información siguiente (si no es legible directamente desde fuera del sensor de movimiento integrado):

— nombre del fabricante del sensor de movimiento integrado,

— número de pieza del fabricante y año de fabricación del sensor de movimiento integrado,

— marca de homologación del sensor de movimiento integrado.

5. INSTALACIÓN DEL APARATO DE CONTROL EQUIPADO CON UN ADAPTADOR

5.1. **Instalación**

ADA_029 Los adaptadores destinados a los vehículos solo podrán ser instalados por los fabricantes de vehículos, o por talleres autorizados para instalar, activar y calibrar tacógrafos digitales y tacógrafos inteligentes.

ADA_030 El taller autorizado que instale el adaptador ajustará la interfaz de entrada y seleccionará el factor de división de la señal de entrada (si procede).

ADA_031 El taller autorizado que instale el adaptador precintará su caja.

ADA_032 El adaptador se colocará lo más cerca posible de la parte del vehículo que proporcione sus impulsos de entrada.

ADA_033 Los cables que alimenten el adaptador serán rojos (carga positiva) y negros (tierra).

5.2. **Precintos**

ADA_034 Serán de aplicación los siguientes requisitos de precintado:

— se precintará la caja del adaptador (véase ADA_017),

— se colocará un precinto entre la caja del sensor integrado y la caja del adaptador, a menos que sea imposible retirar el sensor integrado sin romper el precinto o los precintos de la caja del adaptador (véase ADA_018),

— se colocará un precinto entre la caja del adaptador y el vehículo,

— la conexión entre el adaptador y el equipo que proporciona sus impulsos de entrada se precintará en ambos extremos (en la medida de lo razonablemente posible).

6. VERIFICACIONES, CONTROLES Y REPARACIONES

6.1. **Controles periódicos**

ADA_035 Cuando se utilice un adaptador, en cada control periódico (controles periódicos son aquellos que se ajustan a los requisitos (409) a (413) del anexo IC) del aparato de control, se verificará lo siguiente:

— si el adaptador lleva las inscripciones de homologación adecuadas,

— si están intactos los precintos del adaptador y sus conexiones,

— si el adaptador está instalado de acuerdo con las indicaciones de la placa de instalación,

— si el adaptador está instalado con arreglo a las especificaciones del fabricante del adaptador o del vehículo,

— si está autorizado el montaje de un adaptador en el vehículo inspeccionado.

ADA_036 Dichos controles deberán incluir un calibrado y una sustitución de todos los precintos, sea cual sea su estado.

7. HOMOLOGACIÓN DEL APARATO DE CONTROL EQUIPADO CON UN ADAPTADOR

7.1. **Aspectos generales**

ADA_037 El aparato de control se presentará completo a la homologación, provisto del adaptador (425).

ADA_038 Todo adaptador podrá presentarse a su propia homologación o a la homologación como componente de un aparato de control.

ADA_039 La homologación incluirá los ensayos funcionales del adaptador. El resultado positivo de cada uno de estos ensayos se consignará en un certificado (426).

7.2. **Certificado funcional**

ADA_040 Se entregará al fabricante del adaptador un certificado funcional del adaptador o del aparato de control provisto de un adaptador una vez superados los siguientes ensayos funcionales mínimos.

N.º	Ensayo	Descripción	Requisitos correspondientes
1.	**Examen administrativo**		
1.1	Documentación	Corrección de la documentación del adaptador	
2.	**Inspección visual**		
2.1.	Conformidad del adaptador con la documentación		
2.2.	Identificación/inscripciones del adaptador		ADA_027, ADA_028
2.3	Materiales del adaptador		(219) a (223) ADA_026
2.4.	Precintos		ADA_017, ADA_018, ADA_034
3.	**Ensayos funcionales**		
3.1	Inducción de los impulsos de velocidad al sensor de movimiento integrado		ADA_013
3.2	Interconexión y adaptación de los impulsos de velocidad de entrada		ADA_011, ADA_012
3.3	Precisión de la medición del movimiento		(30) a (35), (217)
4.	**Ensayos ambientales**		
4.1	Resultados de ensayo del fabricante	Resultados de los ensayos ambientales del fabricante.	ADA_020, ADA_021, ADA_022, ADA_024
5.	**EMC**		
5.1	Emisiones radiadas y susceptibilidad	Verificar cumplimiento de la Directiva 2006/28/CE	ADA_024
5.2	Resultados de ensayo del fabricante	Resultados de los ensayos ambientales del fabricante.	ADA_024