DECISIÓN DE EJECUCIÓN (UE) 2015/1505 DE LA COMISIÓN

de 8 de septiembre de 2015

por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE ([1]), y, en particular, su artículo 22, apartado 5,

Considerando lo siguiente:

(1) Las listas de confianza son esenciales para la creación de un clima de confianza entre los operadores del mercado, ya que indican la cualificación del proveedor de servicios en el momento de la supervisión.

(2) El uso transfronterizo de firmas electrónicas ha sido facilitado en virtud de la Decisión 2009/767/CE de la Comisión ([2]), que impone a los Estados miembros la obligación de establecer, mantener y publicar listas de confianza que incluyan información referida a los proveedores de servicios de certificación que expiden certificados cualificados al público de conformidad con la Directiva 1999/93/CE del Parlamento Europeo y del Consejo ([3]) y que estén supervisadas y acreditadas por los Estados miembros.

(3) El artículo 22 del Reglamento (UE) nº 910/2014 impone a los Estados miembros la obligación de establecer, mantener y publicar listas de confianza, de manera segura, firmadas o selladas electrónicamente en una forma apropiada para el tratamiento automático y de notificar a la Comisión los organismos responsables del establecimiento de las listas de confianza nacionales.

(4) Un proveedor de servicios de confianza y los servicios de confianza que ofrece deben considerarse cualificados cuando la cualificación se ha asociado con el proveedor en la lista de confianza. Con el fin de garantizar que los proveedores de servicios puedan cumplir fácilmente las demás obligaciones derivadas del Reglamento (UE) nº 910/2014, en particular las establecidas en los artículos 27 y 37, a distancia y por medios electrónicos, y con el fin de responder a las expectativas legítimas de otros proveedores de servicios de certificación que no expidan certificados cualificados, pero que ofrezcan servicios relacionados con las firmas electrónicas en el marco de la Directiva 1999/93/CE y que se incluyan en la lista antes del 30 de junio de 2016, los Estados miembros deben poder añadir servicios de confianza distintos de los cualificados en las listas de confianza, de manera voluntaria, a escala nacional y siempre que se indique claramente que no están cualificados de conformidad con el Reglamento (UE) nº 910/2014.

(5) Conforme al considerando 25 del Reglamento (UE) nº 910/2014, los Estados miembros podrán añadir otros tipos de servicios de confianza definidos a escala nacional distintos de los definidos en el artículo 3, apartado 16, del Reglamento (UE) nº 910/2014, siempre que esté claramente indicado que no están cualificados de conformidad con el Reglamento (UE) nº 910/2014.

(6) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité establecido por el artículo 48 del Reglamento (UE) nº 910/2014.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Los Estados miembros establecerán, publicarán y mantendrán listas de confianza que incluyan información sobre los proveedores de servicios de confianza cualificados que supervisan, así como información sobre los servicios de confianza cualificados que proporcionan dichos proveedores. Esas listas se ajustarán a las especificaciones técnicas que figuran en el anexo I.

([1]) DO L 257 de 28.8.2014, p. 73.

([2]) Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las «ventanillas únicas» con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo, relativa a los servicios en el mercado interior (DO L 274 de 20.10.2009, p. 36).

([3]) Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (DO L 13 de 19.1.2000, p. 12).

Artículo 2

Los Estados miembros podrán incluir en las listas de confianza información sobre proveedores de servicios de confianza no cualificados, junto con información relacionada con los servicios de confianza no cualificados que proporcionan. La lista deberá indicar claramente qué proveedores de servicios de confianza no están cualificados y cuáles son los servicios de confianza que proporcionan que no están cualificados.

Artículo 3

1. De conformidad con el artículo 22, apartado 2, del Reglamento (UE) nº 910/2014, los Estados miembros firmarán o sellarán electrónicamente en una forma apropiada para el tratamiento automático la lista de confianza de acuerdo con las especificaciones técnicas que figuran en el anexo I.

2. Si un Estado miembro publica electrónicamente una versión legible por personas de la lista de confianza, se asegurará de que esa versión de la lista de confianza contenga los mismos datos que la versión apropiada para el tratamiento automático y procederá a firmarla o sellarla por medios electrónicos, de conformidad con las especificaciones técnicas que figuran en el anexo I.

Artículo 4

1. Los Estados miembros notificarán a la Comisión la información a que se refiere el artículo 22, apartado 3, del Reglamento (UE) nº 910/2014 mediante la plantilla incluida en el anexo II.

2. La información a que se refiere el apartado 1 incluirá dos o más certificados de clave pública del operador del sistema, con un desfase mínimo de tres meses entre sus períodos de vigencia, que correspondan a las claves privadas que pueden utilizarse para firmar o sellar electrónicamente la versión apropiada para el tratamiento automático de la lista de confianza y la versión legible por personas cuando se publique.

3. De conformidad con el artículo 22, apartado 4, del Reglamento (UE) nº 910/2014, la Comisión pondrá a disposición del público, a través de un canal seguro a un servidor web autenticado, la información a que se refieren los apartados 1 y 2 que hayan notificado los Estados miembros, en una versión firmada o sellada electrónicamente apropiada para el tratamiento automático.

4. La Comisión podrá poner a disposición del público, a través de un canal seguro a un servidor web autenticado, la información a que se refieren los apartados 1 y 2 que hayan notificado los Estados miembros, en una forma firmada o sellada legible por personas.

Artículo 5

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

La presente Decisión será obligatoria en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 8 de septiembre de 2015.

Por la Comisión

El Presidente

Jean-Claude JUNCKER

ANEXO I

ESPECIFICACIONES TÉCNICAS DE UNA PLANTILLA COMÚN DE LISTAS DE CONFIANZA

CAPÍTULO I

REQUISITOS GENERALES

Las listas de confianza deberán incluir información tanto actual como histórica, desde la fecha de inclusión de un proveedor de servicios de confianza en las listas de confianza, acerca del estado de los servicios de confianza incluidos en la lista.

Los términos «aprobado», «acreditado» y «supervisado» utilizados en las presentes especificaciones también comprenden los sistemas de aprobación nacionales, pero los Estados miembros proporcionarán información adicional sobre la naturaleza de tales sistemas nacionales en su lista de confianza, incluida una aclaración con respecto a las posibles diferencias con los sistemas de supervisión aplicados a los proveedores de servicios de confianza cualificados y a los servicios de confianza cualificados que estos prestan.

La información que se proporciona en la lista de confianza está destinada principalmente a respaldar la validación de los *tokens* de servicios de confianza cualificados, es decir, objetos físicos o binarios (lógicos) generados o expedidos como resultado de la utilización de un servicio de confianza cualificado, por ejemplo, firmas electrónicas o sellos electrónicos cualificados, firmas electrónicas o sellos electrónicos avanzados admitidos por un certificado cualificado, marcas de tiempo cualificadas, pruebas de entrega electrónica cualificadas, etc.

CAPÍTULO II

ESPECIFICACIONES DETALLADAS DE LA PLANTILLA COMÚN DE LAS LISTAS DE CONFIANZA

Las presentes especificaciones se basan en las especificaciones y los requisitos establecidos en la norma ETSI TS 119 612 v2.1.1 (denominada en lo sucesivo ETSI TS 119 612).

Cuando en las presentes especificaciones no se establezca ningún requisito específico, se aplicarán íntegramente los requisitos de las cláusulas 5 y 6 de ETSI TS 119 612. Cuando se establezcan requisitos específicos, estos prevalecerán sobre los requisitos correspondientes de ETSI TS 119 612. En caso de discrepancia entre las presentes especificaciones y las especificaciones de ETSI TS 119 612, prevalecerán las primeras.

Scheme name (cláusula 5.3.6)

Este campo deberá estar presente y cumplir las especificaciones previstas en la cláusula 5.3.6 de TS 119 612, y se utilizará para el sistema el nombre que sigue:

«EN_name_value» = «Lista de confianza que incluye información relacionada con los proveedores de servicios de confianza cualificados que supervisa el Estado miembro de expedición, junto con información relacionada con los servicios de confianza cualificados que estos prestan, de conformidad con las disposiciones pertinentes establecidas en el Reglamento nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE».

Scheme information URI (cláusula 5.3.7)

Este campo deberá estar presente y cumplir las especificaciones previstas en la cláusula 5.3.7 de TS 119 612, y la «información apropiada sobre el sistema» incluirá, al menos:

a) Información introductoria común a todos los Estados miembros con respecto al alcance y al contexto de la lista de confianza, el sistema de supervisión subyacente y, en su caso, los sistemas de aprobación (por ejemplo, acreditación) nacionales aplicables. El texto común que debe utilizarse es el que figura a continuación, en el que la cadena de caracteres «[*nombre del Estado miembro pertinente*]» será sustituida por el nombre del Estado miembro pertinente:

> «La presente lista es la lista de confianza que incluye información relacionada con los proveedores de servicios de confianza cualificados supervisados por [*nombre del Estado miembro pertinente*], junto con información relacionada con los servicios de confianza cualificados que estos prestan, de conformidad con las disposiciones pertinentes establecidas en el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

El uso transfronterizo de firmas electrónicas ha sido facilitado en virtud de la Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, que estipula la obligación de los Estados miembros de establecer, mantener y publicar listas de confianza que incluyan información referida a los proveedores de servicios de certificación que expiden certificados cualificados al público de conformidad con la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, y que estén supervisados y acreditados por los Estados miembros. La presente lista de confianza es la continuación de la lista de confianza establecida por la Decisión 2009/767/CE».

Las listas de confianza son elementos esenciales para la creación de un clima de confianza entre los operadores del mercado electrónico, puesto que permiten a los usuarios determinar el estado de cualificado y el historial de estado de los proveedores de servicios de confianza y de sus servicios.

Las listas de confianza de los Estados miembros incluyen, como mínimo, la información especificada en los artículos 1 y 2 de la Decisión 2015/[reemplazar con el número de la presente Decisión de Ejecución (UE) 2015/1505 de la Comisión.

Los Estados miembros podrán incluir en las listas de confianza información sobre proveedores de servicios de confianza no cualificados, junto con información relacionada con los servicios de confianza no cualificados que proporcionan. Se indicará claramente que no están cualificados de conformidad con el Reglamento (UE) nº 910/2014.

Los Estados miembros podrán incluir en las listas de confianza información sobre otros tipos de servicios de confianza definidos a escala nacional distintos de los definidos en el artículo 3, apartado 16, del Reglamento (UE) nº 910/2014. Se indicará claramente que no están cualificados de conformidad con el Reglamento (UE) nº 910/2014.

b) Información específica sobre el sistema de supervisión subyacente y, en su caso, los sistemas de aprobación (por ejemplo, acreditación) nacionales aplicables, en particular ([1]):

1) información sobre el sistema de supervisión nacional aplicable a proveedores de servicios de confianza cualificados y no cualificados y a los servicios de confianza cualificados y no cualificados que estos presten, según lo regula el Reglamento (UE) nº 910/2014;

2) información, en su caso, sobre los sistemas de acreditación voluntaria nacionales aplicables a proveedores de servicios de certificación que han expedido certificados cualificados de conformidad con la Directiva 1999/93/CE.

Esta información específica incluirá, como mínimo, para cada sistema subyacente enumerado:

1) una descripción general;

2) información sobre el proceso seguido para el sistema de supervisión nacional y, en su caso, para la aprobación en el marco de un sistema de aprobación nacional;

3) información sobre los criterios que se siguen para supervisar o, en su caso, aprobar a los proveedores de servicios de confianza;

4) información sobre los criterios y normas que se utilizan para seleccionar los supervisores y auditores y definir cómo se evalúa a los proveedores de servicios de confianza y los servicios de confianza que estos prestan;

5) en su caso, otra información de contacto y general aplicable al funcionamiento del sistema.

Scheme type/community/rules (cláusula 5.3.9)

Este campo deberá estar presente y cumplir las especificaciones previstas en la cláusula 5.3.9 de TS 119 612.

Solo deberá incluir URI en inglés del Reino Unido.

([1]) Esos conjuntos de información son de vital importancia para que las partes usuarias evalúen el nivel de calidad y seguridad de tales sistemas. Estos conjuntos de información se facilitarán en el nivel de la lista de confianza mediante el uso del presente «Scheme information URI» (cláusula 5.3.7 — información facilitada por el Estado miembro), de «Scheme type/community/rules» (cláusula 5.3.9 — mediante el uso de un texto común a todos los Estados miembros) y de «TSL policy/legal notice» (cláusula 5.3.11 — texto común a todos los Estados miembros, junto con la posibilidad de que cada Estado miembro añada textos/referencias específicas). Se podrá proporcionar información adicional sobre tales sistemas sobre servicios de confianza no cualificados y servicios de confianza (cualificados) definidos a escala nacional en el nivel de servicio cuando sea aplicable y necesario (por ejemplo, para distinguir entre varios niveles de calidad o de seguridad) a través del uso de «Scheme service definition URI» (cláusula 5.5.6).

Deberá incluir al menos dos URI:

1) Un URI común a todas las listas de confianza de los Estados miembros que lleve a un texto descriptivo que será aplicable a todas las listas de confianza:

URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

Texto descriptivo:

«Participation in a scheme

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

Policy/rules for the assessment of the listed services

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (UE) 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The "qualified" status of a trust service is indicated by the combination of the "Service type identifier" ("Sti") value in a service entry and the status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time". Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A "CA/QC" "Service type identifier" ("Sti") entry (possibly further qualified as being a "RootCA-QC" through the use of the appropriate "Service information extension" ("Sie") additionalServiceInformation Extension)

— indicates that any end-entity certificate issued by or under the CA represented by the "Service digital identifier" ("Sdi") CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

  — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

  — the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. "undersupervision", "supervisionincessation", "accredited" or "granted") for that entry.

— **and IF** "Sie" "Qualifications Extension" information is present, then in addition to the above default rule, those certificates that are identified through the use of "Sie" "Qualifications Extension" information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the "SSCD support" and/or "Legal person as subject" (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific "Key usage" pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of "Qualifiers" used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

  — to indicate the qualified certificate nature:

    — "QCStatement" meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;

    — "QCForESig" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (UE) nº 910/2014;

    — "QCForESeal" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (UE) nº 910/2014;

    — "QCForWSA" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (UE) nº 910/2014.

  — to indicate that the certificate is not to be considered as qualified:

    — "NotQualified" meaning the identified certificate(s) is(are) not to be considered as qualified; and/or

  — to indicate the nature of the SSCD support:

    — "QCWithSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

    — "QCNoSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

    — "QCSSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

  — to indicate the nature of the QSCD support:

    — "QCWithQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

    — "QCNoQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

    — "QCQSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

    — "QCQSCDManagedOnBehalf" indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or

— to indicate issuance to Legal Person:

— "QCForLegalPerson" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and

— if no "Sie" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "QCStatement" qualifier, or

— an "Sie" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "NotQualified" qualifier,

then the certificate is not to be considered as qualified.

"Service digital identifiers" are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other "Sti" type entry is that, for that "Sti" identified service type, the listed service named according to the "Service name" field value and uniquely identified by the "Service digital identity" field value has the current qualified or approval status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time".

Specific interpretation rules for any additional information with regard to a listed service (e.g. "Service information extensions" field) may be found, when applicable, in the Member State specific URI as part of the present "Scheme type/community/rules" field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.»

2) Un URI específico de la lista de confianza del Estado miembro que lleve a un texto descriptivo que será aplicable a la lista de confianza de este Estado miembro:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, donde CC = el código de país ISO 3166-1 ([1]) alfa-2 utilizado en el campo «Scheme territory» (cláusula 5.3.10)

— donde los usuarios pueden obtener las normas y políticas específicas del Estado miembro a las que se hace referencia que se siguen en la evaluación de los servicios de confianza incluidos en la lista, en cumplimiento del sistema de supervisión y, en su caso, del sistema de aprobación del Estado miembro,

— donde los usuarios pueden obtener la descripción concreta del Estado miembro a la que se hace referencia acerca de cómo utilizar e interpretar el contenido de la lista de confianza con respecto a los servicios de confianza no cualificados que figuran en la lista y los servicios de confianza definidos a nivel nacional. Esto podrá utilizarse para indicar una granularidad potencial en el sistema de aprobación nacional en relación con los CSP que no expiden QC y cómo se utilizan a tal efecto los campos «Scheme service definition URI» (cláusula 5.5.6) y «Service información extension» (cláusula 5.5.9).

Los Estados miembros PODRÁN definir y utilizar URI adicionales que amplíen el URI específico del Estado miembro (es decir, URI definidos a partir de este URI específico jerárquico).

TSL policy/legal notice (cláusula 5.3.11)

Este campo deberá estar presente y cumplir las especificaciones de la cláusula 5.3.11 de TS 119 612 en virtud de la cual la política o el aviso legal referente a la situación jurídica del sistema o los requisitos legales que cumple el sistema en virtud de la jurisdicción en el que se ha establecido y/o las restricciones y condiciones en virtud de las cuales se mantiene y publica la lista de confianza deben ser una secuencia de cadenas de caracteres multilingües (véase la

([1]) ISO 3166-1:2006: «Códigos para la representación de nombres de países y sus subdivisiones. Parte 1: Códigos de los países».

cláusula 5.1.4) que proporcione, en inglés del Reino Unido como lengua obligatoria y de manera opcional en una o más lenguas nacionales, el texto real de tal política o aviso de la manera siguiente:

1) una primera parte obligatoria, común a las listas de confianza de todos los Estados miembros, que indique el marco jurídico aplicable, y cuya versión en inglés es la siguiente:

> The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Texto en la lengua nacional de un Estado miembro:

> El marco jurídico aplicable a la presente lista de confianza es el Reglamento nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

2) Una segunda parte opcional, específica para cada lista de confianza, que indique las referencias a marcos jurídicos nacionales concretos aplicables.

Service current status (cláusula 5.5.4)

Este campo deberá estar presente y cumplir las especificaciones previstas en la cláusula 5.5.4 de TS 119 612.

La migración del valor de «Service current status» de los servicios que figuran en la lista de confianza EUMS con fecha del día anterior a la de la aplicación del Reglamento (UE) nº 910/2014 (es decir, el 30 de junio de 2016) se llevará a cabo el día en que se aplique el Reglamento (es decir, el 1 de julio de 2016), tal y como se especifica en el anexo J de ETSI TS 119 612.

CAPÍTULO III

CONTINUIDAD DE LAS LISTAS DE CONFIANZA

Los certificados que se notificarán a la Comisión de conformidad con el artículo 4, apartado 2, de la presente Decisión deberán cumplir los requisitos de la cláusula 5.7.1 de ETSI TS 119 612 y se expedirán de manera que:

— tengan por lo menos tres meses de diferencia en su fecha final de validez («Not After»),

— se creen en pares de claves nuevos; los pares de claves utilizados anteriormente no se deben volver a certificar.

En caso de expiración de uno de los certificados de clave pública que se podrían utilizar para validar la firma o el sello de la lista de confianza que se ha notificado a la Comisión y que se ha publicado en la lista central de indicadores de la Comisión, los Estados miembros:

— en el caso de que la lista de confianza actualmente publicada haya sido firmada o sellada con una clave privada cuyo certificado de clave pública haya expirado, reexpedirán, sin demora, una nueva lista de confianza firmada o sellada con una clave privada cuyo certificado de clave pública notificado no haya expirado,

— cuando sea necesario, generarán nuevos pares de claves que se podrían usar para firmar o sellar la lista de confianza y realizarán la generación de sus correspondientes certificados de clave pública,

— notificarán de inmediato a la Comisión la nueva lista de certificados de clave pública correspondientes a las claves privadas que podrían utilizarse para firmar o sellar la lista de confianza.

En el caso de que una de las claves privadas correspondiente a uno de los certificados de clave pública que se podrían usar para validar la firma o el sello de la lista de confianza, que se ha notificado a la Comisión y que se ha publicado en la lista central de indicadores de la Comisión, se vea comprometida o sea retirada, los Estados miembros:

— reexpedirán, sin demora, una nueva lista de confianza firmada o sellada con una clave privada no comprometida en caso de que la lista de confianza publicada se haya firmado o sellado con una clave privada comprometida o retirada,

— cuando sea necesario, generarán nuevos pares de claves que se podrían usar para firmar o sellar la lista de confianza y realizarán la generación de sus correspondientes certificados de clave pública,

— notificarán de inmediato a la Comisión la nueva lista de certificados de clave pública correspondientes a las claves privadas que podrían utilizarse para firmar o sellar la lista de confianza.

En caso de que se comprometan o se retiren todas las claves privadas correspondientes a los certificados de clave pública que podrían utilizarse para validar la firma de la lista de confianza, que se hayan notificado a la Comisión y que figuren publicadas en la lista central de indicadores de la Comisión, los Estados miembros:

— generarán nuevos pares de claves que se podrían usar para firmar o sellar la lista de confianza y realizarán la generación de sus correspondientes certificados de clave pública,

— reexpedirán, sin demora, una nueva lista de confianza firmada o sellada con una de esas nuevas claves privadas, y cuyo certificado de clave pública correspondiente deba ser notificado,

— notificarán de inmediato a la Comisión la nueva lista de certificados de clave pública correspondientes a las claves privadas que podrían utilizarse para firmar o sellar la lista de confianza.

CAPÍTULO IV

ESPECIFICACIONES PARA LA FORMA LEGIBLE POR PERSONAS DE LA LISTA DE CONFIANZA

Si se establece y se publica una forma legible por personas de la lista de confianza, deberá facilitarse en forma de documento PDF con arreglo a ISO 32000 ([1]), que deberá estar formateado de acuerdo con el perfil PDF/A (ISO 19005 ([2])).

El contenido de la forma legible por personas basada en PDF/A de la lista de confianza deberá cumplir los siguientes requisitos:

— La estructura de la forma legible por personas deberá reflejar el modelo lógico descrito en TS 119 612.

— Deberán aparecer todos los campos presentes, que facilitarán:

  — el título del campo (por ejemplo, «Service type identifier»),

  — el valor del campo (por ejemplo, «http://uri.etsi.org/TrstSvc/Svctype/CA/QC»),

  — el significado (descripción) del valor del campo, cuando corresponda (por ejemplo, «Un servicio de generación de certificados que crea y firma certificados cualificados en función de la identidad y otros atributos verificados por los servicios de registro pertinentes»),

  — varias versiones en lenguajes naturales según lo previsto en la lista de confianza, si procede.

— Los siguientes campos y los valores correspondientes de los certificados digitales ([3]), si están presentes en el campo «Service digital identity», se mostrarán, como mínimo, en versión legible por personas:

  — versión,

  — número de serie del certificado,

  — algoritmo de firma,

  — expedidor: todos los campos con denominación distinguida pertinentes,

  — período de validez,

  — sujeto: todos los campos con denominación distinguida pertinentes,

([1]) ISO 32000-1:2008: Gestión de documentos — PDF — Parte 1: PDF 1.7.
([2]) ISO 19005-2:2011: Gestión de documentos — Formato de archivo de documento electrónico para su conservación a largo plazo — Parte 2: Uso de ISO 32000-1 (PDF/A-2).
([3]) Recomendación ITU-T X.509 | ISO/IEC 9594-8: Tecnología de la información-Interconexión de sistemas abiertos-El Directorio: marcos de certificados de atributos y clave pública (véase http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509)

— clave pública,

— identificador de clave de autoridad,

— identificador de clave de sujeto,

— uso de claves,

— uso de claves extendido,

— políticas de certificado: todos los identificadores y calificadores de políticas,

— correlaciones de políticas,

— nombre alternativo del sujeto,

— atributos de directorio del sujeto,

— restricciones básicas,

— restricciones políticas,

— puntos de distribución CRL ([1]),

— acceso a la información de autoridad,

— acceso a la información de sujeto,

— declaraciones de certificados cualificados ([2]),

— algoritmo de comprobación aleatoria,

— valor de comprobación aleatoria de certificado.

— La versión legible por personas se deberá poder imprimir fácilmente.

— La versión legible por personas deberá estar firmada o sellada por el operador del sistema de conformidad con la firma avanzada de PDF especificada en los artículos 1 y 3 de la Decisión de Ejecución (UE) 2015/1505 de la Comisión.

([1]) RFC 5280: Certificado PKI y perfil CRL X.509 de internet.
([2]) RFC 3739: PKI X.509 de internet: perfil de certificados reconocidos.

ANEXO II

PLANTILLA PARA LAS NOTIFICACIONES DE LOS ESTADOS MIEMBROS

La información que deben notificar los Estados miembros de conformidad con el artículo 4, apartado 1, de la presente Decisión deberá contener los siguientes datos y cualesquiera modificaciones de los mismos:

1) Estado miembro, con códigos alfa 2 conforme a la norma ISO 3166-1 ([1]), con las siguientes excepciones:

   a) El código de país para el Reino Unido será «UK».

   b) El código de país para Grecia será «EL».

2) El organismo o los organismos responsables del establecimiento, el mantenimiento y la publicación de la versión apropiada para el tratamiento automático y la versión legible por personas de las listas de confianza:

   a) Scheme operator name (nombre del operador del sistema): la información facilitada debe ser idéntica (respetando las mayúsculas y minúsculas) al valor «Scheme operator name» que figura en la lista de confianza en todas las lenguas que se utilicen en dicha lista.

   b) Información opcional para uso interno de la Comisión solo en los casos en que se deba contactar con el organismo de que se trate (la información no se publicará en la lista compilada por la CE de listas de confianza):

      — dirección del operador del sistema;

      — detalles de contacto de las personas responsables (nombre, teléfono, dirección de correo electrónico).

3) Lugar en que esté publicada la versión apropiada para el tratamiento automático de la lista de confianza (*lugar en que está publicada la lista de confianza actual*).

4) Lugar en que esté publicada una versión de la lista de confianza legible por personas (*lugar en que está publicada la lista de confianza actual*). En caso de que ya no esté publicada una lista de confianza legible por personas, una indicación de este hecho.

5) Los certificados de clave pública que corresponden a las claves privadas que se pueden utilizar para firmar o sellar electrónicamente la versión apropiada para el tratamiento automático de la lista de confianza y la versión legible por personas de las listas de confianza: los certificados se proporcionarán como certificados DER con codificación Base64 de Privacy-enhanced Mail. Para notificar cambios, se debe añadir información adicional en caso de que un nuevo certificado deba sustituir al certificado específico de la lista de la Comisión y en el caso de que el certificado notificado se deba añadir a los existentes sin ninguna sustitución.

6) Fecha de presentación de los datos notificados en los puntos 1 a 5.

Los datos notificados con arreglo a los puntos 1, 2, letra a), 3, 4 y 5 se incluirán en la lista compilada por la CE de listas de confianza en sustitución de la información notificada previamente incluida en esa lista compilada.

([1]) ISO 3166-1: «Códigos para la representación de nombres de países y sus subdivisiones. Parte 1: Códigos de los países».