Este documento es un instrumento de documentación y no compromete la responsabilidad de las instituciones

►**B** ►**C1** **DECISIÓN 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

[notificada con el número C(2009) 7806]

(Texto pertinente a efectos del EEE)

(2009/767/CE) ◄

(DO L 274 de 20.10.2009, p. 36)

Modificado por:

		Diario Oficial		
		n°	página	fecha
►**M1**	Decisión 2010/425/UE de la Comisión de 28 de julio de 2010	L 199	30	31.7.2010

Rectificada por:

►**C1** Rectificación, DO L 299 de 14.11.2009, p. 18 (2009/767/CE)
►**C2** Rectificación, DO L 4 de 7.1.2011, p. 6 (2009/767/CE)

▼B
▼C1

DECISIÓN 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

[notificada con el número C(2009) 7806]

(Texto pertinente a efectos del EEE)

(2009/767/CE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea,

Vista la Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior [1], y, en particular, su artículo 8, apartado 3,

Considerando lo siguiente:

(1) Las obligaciones de simplificación administrativa impuestas a los Estados miembros en el capítulo II de la Directiva 2006/123/CE, y, en particular, en sus artículos 5 y 8, incluyen la obligación de simplificar los procedimientos y trámites aplicables al acceso a actividades de servicios y su ejercicio y la obligación de garantizar que los prestadores de servicios puedan realizar fácilmente dichos procedimientos y trámites a distancia y por vía electrónica, a través de las «ventanillas únicas».

(2) La realización de los procedimientos y trámites a través de las «ventanillas únicas» debe ser posible a través de las fronteras entre Estados miembros con arreglo al artículo 8 de la Directiva 2006/123/CE.

(3) Para respetar la obligación de simplificar los procedimientos y trámites y facilitar el uso transfronterizo de las «ventanillas únicas», los procedimientos por vía electrónica deben basarse en soluciones sencillas, en particular en lo que se refiere al uso de firmas electrónicas. En los casos en que, tras una adecuada evaluación del riesgo de los procedimientos y trámites concretos, se considere necesario un nivel elevado de seguridad o una equivalencia con la firma manuscrita, podrían exigirse a los prestadores de servicios, para determinados procedimientos y trámites, firmas electrónicas avanzadas basadas en un certificado reconocido, con o sin dispositivo seguro de creación de firma.

[1] DO L 376 de 27.12.2006, p. 36.

▼C1

(4) El marco comunitario de la firma electrónica se creó en 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 ([1]). A fin de que del uso transfronterizo de las firmas electrónicas avanzadas basadas en un certificado reconocido resulte eficaz, debe reforzarse la confianza en estas firmas electrónicas con independencia del Estado miembro en que esté establecido el firmante o el proveedor de servicios de certificación que expida el certificado reconocido. Esto podría conseguirse ofreciendo más fácilmente en una forma confiable la información necesaria para validar las firmas electrónicas, y en particular la información relativa a los proveedores de servicios de certificación que están supervisados/acreditados en un Estado miembro y a los servicios que prestan.

(5) Es necesario garantizar que los Estados miembros pongan esta información a disposición del público mediante un modelo común, a fin de facilitar su uso y garantizar un nivel de detalle apropiado que permita a la parte receptora validar la firma electrónica.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Uso y aceptación de firmas electrónicas

1. Si se justifica sobre la base de una evaluación apropiada de los riesgos existentes y de conformidad con el artículo 5, apartados 1 y 3, de la Directiva 2006/123/CE, los Estados miembros podrán exigir, para la realización de algunos procedimientos y trámites a través de las ventanillas únicas con arreglo al artículo 8 de la Directiva 2006/123/CE, el uso por el prestador del servicio de firmas electrónicas avanzadas basadas en un certificado reconocido, con o sin dispositivo seguro de creación de firma, según se definen y regulan en la Directiva 1999/93/CE.

2. Los Estados miembros aceptarán cualquier firma electrónica avanzada basada en un certificado reconocido, con o sin dispositivo seguro de creación de firma, para la realización de los procedimientos y trámites a que se refiere el apartado 1, sin perjuicio de la posibilidad de que los Estados miembros limiten esta aceptación a las firmas electrónicas avanzadas basadas en un certificado reconocido y creadas mediante un dispositivo seguro de creación de firma si ello está en consonancia con la evaluación del riesgo a que se refiere el apartado 1.

3. Los Estados miembros no supeditarán la aceptación de las firmas electrónicas avanzadas basadas en un certificado reconocido, con o sin dispositivo seguro de creación de firma, a requisitos que obstaculicen el uso, por los prestadores de servicios, de procedimientos por vía electrónica a través de las ventanillas únicas.

([1]) DO L 13 de 19.1.2000, p. 12.

▼C1

4. El apartado 2 no impedirá a los Estados miembros aceptar firmas electrónicas distintas de las firmas electrónicas avanzadas basadas en un certificado reconocido, con o sin dispositivo seguro de creación de firma.

Artículo 2

Establecimiento, mantenimiento y publicación de listas de confianza

1. Cada Estado miembro establecerá, mantendrá y publicará, de conformidad con las especificaciones técnicas que figuran en el anexo, una «lista de confianza» que contenga la información mínima referente a los proveedores de servicios de certificación que expiden certificados reconocidos al público por él supervisados/acreditados.

▼M1

2. Los Estados miembros elaborarán y publicarán una versión de la lista de confianza legible por personas y otra versión procesable por máquina, de conformidad con las especificaciones que figuran en el anexo.

2 *bis*. Los Estados miembros firmarán electrónicamente la versión procesable por máquina de sus respectivas listas de confianza y publicarán, como mínimo, una versión de las mismas legible por las personas a través de un canal seguro a fin de garantizar su autenticidad e integridad.

3. Los Estados miembros notificarán a la Comisión la siguiente información:

a) el organismo o los organismos responsables del establecimiento, el mantenimiento y la publicación de las versiones de su lista de confianza legible por personas y procesable por máquina;

b) los lugares donde se hallan publicadas las versiones de su lista de confianza legible por personas y procesable por máquina;

c) el certificado de clave pública utilizado para establecer el canal seguro a través del cual se publica la versión de la lista de confianza legible por personas o, si la lista legible por personas ha sido firmada electrónicamente, el certificado de clave pública utilizado para firmarla;

d) el certificado de clave pública utilizado para firmar electrónicamente la versión de la lista de confianza procesable por máquina;

e) cualquier cambio introducido en la información indicada en las letras a) a d).

4. La Comisión pondrá a disposición de los Estados miembros, a través de un canal seguro, en un servidor web autenticado, la información mencionada en el apartado 3 que haya sido comunicada por los Estados miembros, tanto en una versión legible por las personas como en una versión procesable por máquina.

▼C1

Artículo 3

Aplicación

La presente Decisión se aplicará a partir del 28 de diciembre de 2009.

Artículo 4

Destinatarios

Los destinatarios de la presente Decisión serán los Estados miembros.

▼C1

ANEXO

ESPECIFICACIONES TÉCNICAS RELATIVAS A UN MODELO COMÚN PARA LA «LISTA DE CONFIANZA DE PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN SUPERVISADOS/ACREDITADOS»

PREFACIO

1. **Generalidades**

La finalidad del modelo común para la «lista de confianza de proveedores de servicios de certificación supervisados/acreditados» de los Estados miembros es establecer un formato común para que cada Estado miembro facilite la información sobre el estado de supervisión/acreditación de los servicios de certificación de los proveedores de servicios de certificación ([1]) (*certification services providers* o CSP) que supervisa/acredita en cuanto al cumplimiento de las disposiciones pertinentes de la Directiva 1999/93/CE. Se incluye la presentación de información histórica sobre el estado de supervisión/acreditación de los servicios de certificación supervisados/acreditados.

La información obligatoria de la lista de confianza (*Trusted List* o TL) deberá incluir un mínimo de información sobre los CSP supervisados/acreditados que expiden certificados reconocidos (*Qualified Certificates* o QC) ([2]) de conformidad con lo dispuesto en la Directiva 1999/93/CE [artículo 3, apartados 2 y 3, y artículo 7, apartado 1, letra a)], incluida información sobre el QC que respalda una firma electrónica y sobre si la firma se crea o no mediante un dispositivo seguro de creación de firma (SSCD) ([3]).

A nivel nacional y con carácter voluntario, podrá incluirse en la lista de confianza información adicional sobre otros CSP supervisados/acreditados que no expidan QC, pero presten servicios relacionados con las firmas electrónicas (por ejemplo, CSP que presten servicios de estampación de fecha y hora y expidan sellos temporales, CSP que expidan certificados no reconocidos, etc.).

El objetivo principal de esta información es facilitar la validación de una firma electrónica reconocida (*Qualified Electronic Signature* o QES) o una firma electrónica avanzada (*Advanced Electronic Signature* o AdES) ([4]) respaldadas por un certificado reconocido ([5]) ([6]).

El modelo común propuesto es compatible con una implementación basada en las especificaciones de ETSI TS 102 231 ([7]) utilizadas en relación con el establecimiento, publicación, localización, acceso, autenticación y fiabilidad de estos tipos de listas.

([1]) Según se define en el artículo 2, punto 11, de la Directiva 1999/93/CE.
([2]) Según se define en el artículo 2, punto 10, de la Directiva 1999/93/CE.
([3]) Según se define en el artículo 2, punto 6, de la Directiva 1999/93/CE.
([4]) Según se define en el artículo 2, punto 2, de la Directiva 1999/93/CE.
([5]) Para referirse a una AdES respaldada por un QC se utiliza en el presente documento el acrónimo «$AdES_{QC}$».
([6]) Nótese que existen diversos servicios electrónicos basados en la AdES simple cuyo uso transfronterizo se vería también facilitado, siempre que los servicios de certificación que los respalden (por ejemplo, la expedición de certificados no reconocidos) formen parte de los servicios supervisados/acreditados cubiertos por un Estado miembro en la parte de información voluntaria de la lista de confianza.
([7]) ETSI TS 102 231 – *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information*.

▼C1

2. **Directrices para la edición de las entradas de la TL**

2.1. *Una lista de confianza centrada en los servicios de certificación supervisados/acreditados*

Los servicios de certificación y los proveedores de servicios de certificación pertinentes en una misma lista

La lista de confianza de un Estado miembro se define como la «lista del estado de supervisión/acreditación de los servicios de certificación de los proveedores de servicios de certificación que están supervisados/acreditados por el Estado miembro de referencia en cuanto al cumplimiento de las disposiciones pertinentes de la Directiva 1999/93/CE».

Esta lista de confianza debe incluir:

— a todos los proveedores de servicios de certificación, según se definen en el artículo 2, punto 11, de la Directiva 1999/93/CE, es decir «la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica»,

— que están supervisados/acreditados en cuanto al cumplimiento de las disposiciones pertinentes de la Directiva 1999/93/CE.

Al examinar las definiciones y disposiciones contenidas en la Directiva 1999/93/CE, en particular en relación con los CSP pertinentes y sus sistemas de supervisión/acreditación voluntaria, cabe distinguir dos grupos de CSP, a saber, los que expiden QC al público (CSP_{QC}), y los que no los expiden, pero prestan «otros servicios (auxiliares) en relación con la firma electrónica»:

— **CSP que expiden QC:**

  — Deben estar supervisados por el Estado miembro en el que están establecidos (si están establecidos en un Estado miembro) y pueden también estar acreditados en cuanto al cumplimiento de lo dispuesto en la Directiva 1999/93/CE, incluidos los requisitos del anexo I (requisitos para los QC), y del anexo II (requisitos de los CSP que expiden QC). Los CSP que expiden QC acreditados en un Estado miembro deben estar cubiertos de todos modos por el sistema de supervisión apropiado de dicho Estado miembro salvo que no estén establecidos en él.

  — El sistema de «supervisión» aplicable (respectivamente, el sistema de «acreditación voluntaria») está definido en la Directiva 1999/93/CE y debe satisfacer los requisitos que en ella figuran, en particular los establecidos en el artículo 3, apartado 3, artículo 8, apartado 1, artículo 11 y considerando 13 [respectivamente, artículo 2, punto 13, artículo 3, apartado 2, artículo 7, apartado 1, letra a), artículo 8, apartado 1, artículo 11 y considerandos 4 y 11 a 13].

— **CSP que no expiden QC:**

  — Pueden estar cubiertos por un sistema de «acreditación voluntaria» (según se define en la Directiva 1999/93/CE y con arreglo a ella) o por un «régimen de aprobación reconocido» definido a nivel nacional y aplicado a ese mismo nivel para la supervisión del cumplimiento de las disposiciones contenidas en la Directiva y posiblemente de las disposiciones nacionales con respecto a la prestación de servicios de certificación (en el sentido del artículo 2, punto 11, de la Directiva).

  — Algunos de los objetos físicos o binarios (lógicos) generados o expedidos de resultas de la prestación de un servicio de certificación podrán gozar de un «reconocimiento» específico por cumplir las disposiciones y requisitos establecidos a nivel nacional, pero es probable que el significado de este «reconocimiento» quede limitado exclusivamente al nivel nacional.

▼C1

La lista de confianza de un Estado miembro deberá facilitar un mínimo de información sobre los CSP supervisados/acreditados que expidan certificados reconocidos al público de conformidad con lo dispuesto en la Directiva 1999/93/CE [artículo 3, apartados 2 y 3, y artículo 7, apartado 1, letra a)], información sobre el QC que respalda la firma electrónica y sobre si la firma se crea o no mediante un dispositivo seguro de creación de firma.

Podrá incluirse en la lista de confianza a nivel nacional y con carácter voluntario información adicional sobre otros servicios supervisados/acreditados de los CSP que no expiden QC al público (por ejemplo, CSP que presten servicios de estampación de fecha y hora y expidan sellos temporales, CSP que expidan certificados no reconocidos, etc.).

La finalidad de la lista de confianza es:

— recoger y presentar información fiable sobre el estado de supervisión/acreditación de los servicios de certificación de los proveedores de servicios de certificación que están supervisados/acreditados por el Estado miembro responsable de establecer y mantener la lista en cuanto al cumplimiento de las disposiciones pertinentes de la Directiva 1999/93/CE,

— facilitar la validación de las firmas electrónicas respaldadas por los servicios de certificación supervisados/acreditados que constan como prestados por los CSP de la lista.

Un conjunto único de valores sobre el estado de supervisión/acreditación

Deberá establecerse y mantenerse una única TL por Estado miembro para indicar el estado de supervisión o acreditación de los servicios de certificación de los CSP que están supervisados/acreditados por el Estado miembro.

El que un servicio esté actualmente supervisado o acreditado forma parte de su estado actual. Además, un estado de supervisión o acreditación puede estar «vigente», «en proceso de suspensión», «suspendido», o incluso «suprimido». A lo largo de su vida, un mismo servicio de certificación podrá pasar de un estado de supervisión a otro de acreditación y viceversa ([1]).

La siguiente figura 1 describe el flujo esperado, para un único servicio de certificación, entre las posibles situaciones de supervisión/acreditación:

([1]) Por ejemplo un proveedor de servicios de certificación establecido en un Estado miembro que presta un servicio de certificación que inicialmente supervisa el Estado miembro (organismo de supervisión), puede, pasado cierto tiempo, decidir someterse a una acreditación voluntaria para el servicio de certificación actualmente supervisado. A la inversa, un proveedor de servicios de certificación establecido en otro Estado miembro puede decidir no abandonar un servicio de certificación acreditado, sino pasarlo del estado de acreditación al de supervisión, por ejemplo, por razones comerciales o económicas.

▼C1

Flujo esperado del estado de supervisión/acreditación de un servicio de un CSP

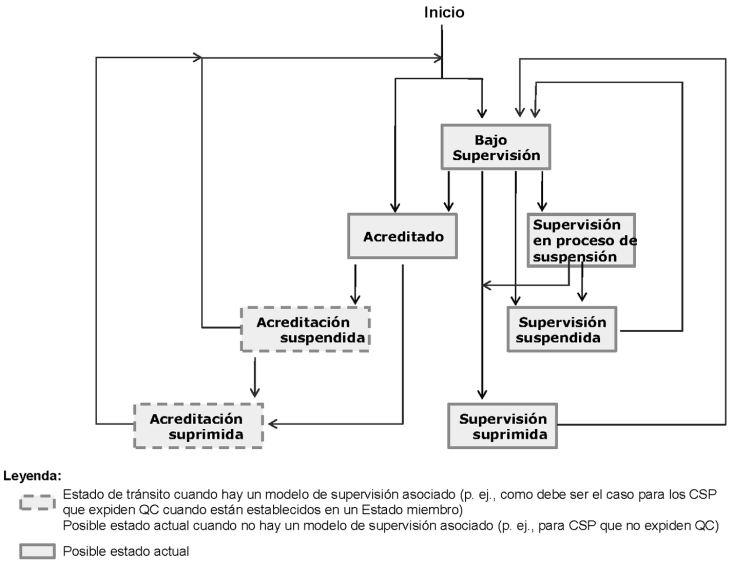


Figura 1

Un servicio de certificación que expida QC deberá ser supervisado (si está establecido en un Estado miembro) y, voluntariamente, podrá ser acreditado. El «valor actual del estado» de tal servicio cuando conste en una lista de confianza puede ser cualquiera de los valores antes indicados. No obstante, conviene señalar que «acreditación suspendida» y «acreditación suprimida» deberán ser solo valores de «estado de tránsito» en el caso de los servicios CSPQC establecidos en un Estado miembro, ya que tales servicios deberán estar supervisados en todo caso (incluso si no están acreditados o han dejado de estarlo).

Los Estados miembros que establezcan o hayan establecido uno o más «regímenes de aprobación reconocidos» definidos y aplicados a nivel nacional para supervisar si los servicios de los CSP que no expiden QC cumplen las disposiciones de la Directiva 1999/93/CE y las eventuales disposiciones nacionales relativas a la prestación de servicios de certificación (en el sentido del artículo 2, punto 11, de la Directiva) deberán clasificar tales regímenes de aprobación en una de las dos categorías siguientes:

— «acreditación voluntaria» según se define y regula en la Directiva 1999/93/CE [artículo 2, punto 13, artículo 3, apartado 2, artículo 7, apartado 1, letra a), artículo 8, apartado 1, artículo 11 y considerandos 4 y 11 a 13],

— «supervisión» según lo exigido en la Directiva 1999/93/CE y aplicado mediante disposiciones y requisitos nacionales de conformidad con el Derecho interno.

▼C1

Por consiguiente, un servicio de certificación que no expida QC podrá ser supervisado o acreditado voluntariamente. El «valor de estado actual» de tal servicio, cuando figure en una lista de confianza, puede ser cualquiera de los valores antes mencionados (véase la figura 1).

La lista de confianza deberá contener información sobre el régimen o los regímenes de supervisión/acreditación subyacentes, y en particular:

— información sobre el sistema de supervisión aplicable a cualquier CSP_{QC},

— información, si procede, sobre el régimen de «acreditación voluntaria» nacional aplicable a cualquier CSP_{QC},

— información, si procede, sobre el sistema de supervisión aplicable a cualquier CSP que no expida QC,

— información, si procede, sobre el régimen de «acreditación voluntaria» nacional aplicable a cualquier CSP que no expida QC.

Los dos últimos elementos de información son de importancia crítica para que las partes usuarias puedan evaluar el nivel de calidad y seguridad de los sistemas de supervisión/acreditación aplicados a nivel nacional a los CSP que no expiden QC. Cuando en la TL figure información sobre el estado de supervisión/acreditación de servicios prestados por CSP que no expiden QC, los elementos de información mencionados deberán facilitarse a nivel de la TL mediante el uso de «Scheme information URI» (cláusula 5.3.7 — información facilitada por los Estados miembros), «Scheme type/community/rules» (cláusula 5.3.9 — mediante el uso de un texto común a todos los Estados miembros, e información específica opcional facilitada por un Estado miembro) y «TSL policy/legal notice» (cláusula 5.3.11 — un texto común a todos los Estados miembros que remite a la Directiva 1999/93/CE, junto con la facultad de cada Estado miembro de añadir texto/referencias específicas propias). Podrá facilitarse a nivel de servicio información adicional sobre «reconocimiento» definida a nivel de los sistemas de supervisión/acreditación nacionales para los CSP que no expiden QC, si procede y es preciso (por ejemplo, para distinguir entre varios niveles de calidad/seguridad), mediante el uso de la extensión «additionalServiceInformation» (cláusula 5.8.2) dentro de la «Service information extension» (cláusula 5.5.9). Se encontrará más información sobre las especificaciones técnicas correspondientes en las especificaciones detalladas del capítulo I.

Pese a que en un Estado miembro pueda haber distintos organismos encargados de la supervisión y acreditación de los servicios de certificación, se espera que se utilice una sola entrada para un mismo servicio de certificación (identificado por su «Service digital identity» con arreglo a ETSI TS 102 231 ([1])) y que su estado de supervisión/acreditación se actualice en consecuencia. El significado de los estados antes mencionados se describe en la cláusula 5.5.4 de las especificaciones técnicas detalladas del capítulo I.

2.2. *Entradas de la TL cuyo objetivo es facilitar la validación de QES y $AdES_{QC}$*

La parte más crítica de la creación de la TL es el establecimiento de su parte obligatoria, a saber, la «lista de servicios» por cada CSP que expide QC, a fin de reflejar correctamente la situación exacta en materia de expedición de cada uno de estos servicios de certificación que expiden QC y de garantizar que la información facilitada en cada entrada sea suficiente para facilitar la validación de QES y $AdES_{QC}$ (cuando se combina con el contenido del QC de entidad final expedido por el CSP dentro del servicio de certificación correspondiente a la entrada).

([1]) ETSI TS 102 231 — *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information*.

▼C1

En la medida en que no existe un perfil del QC verdaderamente interoperable y transfronterizo, la información exigida podría incluir información distinta de la «Service digital identity» de una única CA (raíz), en particular información que identifique la calidad de QC del certificado expedido, y si las firmas respaldadas están o no creadas mediante un SSCD. El organismo de un Estado miembro designado para establecer, editar y mantener la TL (es decir, el operador del régimen según ETSI TS 102 231) deberá tener en cuenta, por tanto, el perfil actual y el contenido del certificado en cada QC expedido, por cada CSP_{QC} incluido en la TL.

Idealmente, cada QC expedido debería incluir la declaración QcCompliance ([1]) definida por el ETSI cuando se afirma que es un QC, así como la declaración QcSSCD definida por el ETSI cuando se afirma que está respaldado por un SSCD para generar firmas electrónicas, o que cada QC expedido incluye uno de los identificadores de objeto (*Object Identifier* o OID) de política de certificados QCP/QCP + definido en ETSI TS 101 456 ([2]). El uso por los CSP que expiden QC de normas distintas como referencias, el amplio margen de interpretación de estas normas y el desconocimiento de la existencia y prioridad de algunas especificaciones técnicas normativas o normas ha provocado diferencias en el contenido real de los QC actualmente expedidos (por ejemplo, el que se usen o no las QcStatements definidas por el ETSI) y, en consecuencia, está impidiendo que las partes receptoras confíen sin más en el certificado del firmante (y en la cadena o trayectoria asociada) para evaluar, al menos de un modo legible por máquina, si se afirma o no que el certificado que avala una firma electrónica es un QC y si está o no asociado con un SSCD mediante el cual se ha creado dicha firma.

Rellenar los campos «Service type identifier» («Sti»), «Service name» («Sn»), y «Service digital identity» («Sdi») ([3]) con la información facilitada en el campo «Service information extensions» («Sie») permite que el modelo común de TL propuesto determine íntegramente un tipo específico de certificado reconocido expedido por un servicio de certificación de un CSP que expide QC que figura en la lista y facilite información sobre si está respaldado o no por un SSCD (cuando tal información está ausente del QC expedido). Por supuesto, con esta entrada está asociada una información específica «Service current status» («Scs»). Todo ello se representa en la figura 2.

El que un servicio figurase en la lista solo con el «Sdi» de una CA (raíz) significaría que está garantizado (por el CSP que expide QC, pero también por el organismo de supervisión/acreditación encargado de la supervisión/acreditación de ese CSP) que cualquier certificado de entidad final expedido bajo esta (jerarquía de) CA (raíz) contiene suficiente información definida por el ETSI y procesable por una máquina para determinar si es un QC o no y si está respaldado por un SSCD. En caso de que, por ejemplo, esto último no sea cierto (es decir que el QC no contenga ninguna indicación procesable por una máquina y normalizada por el ETSI sobre si está respaldada por un SSCD), la inclusión en la lista solo del «Sdi» de esa CA (raíz) solo permite asumir que un QC expedido bajo esta (jerarquía de) CA (raíz) no está respaldado por ningún SSCD. Para considerar esos QC respaldados por un SSCD, debería utilizarse el «Sie» para indicarlo (esto indica también que está garantizado por el CSP que expide los QC y está supervisado/acreditado por el organismo de supervisión o acreditación respectivamente).

([1]) Remitirse a ETSI TS 101 862 — *Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.*

([2]) ETSI TS 101 456 — *Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.*

([3]) Es decir, y como mínimo, un certificado X.509 v3 de la QCA expedidora o de una CA que ocupe una posición más elevada en la trayectoria de certificación.

▼C1

Principios generales — Reglas de edición — Entradas CSP_{QC} (servicios de la lista)

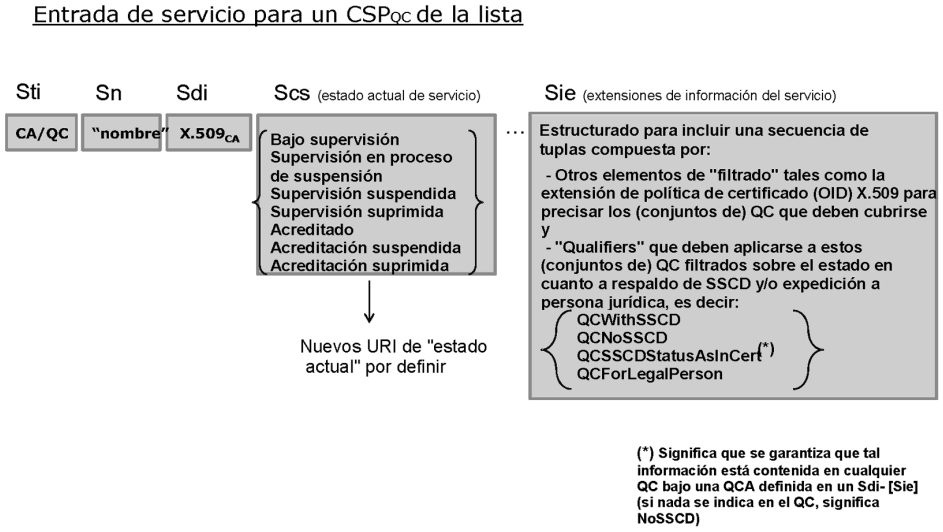


Figura 2

Entrada de un servicio de un CSP que expide QC de la lista en la TL implementada en formato TSL

Las presentes especificaciones técnicas del modelo común de la TL permiten utilizar una combinación de cinco partes principales de información en la entrada del servicio:

— el «Service type identifier» («Sti»), por ejemplo para identificar una CA que expide QC («CA/QC»),

— el «Service name» («Sn»),

— la información «Service digital identity» («Sdi») que identifica un servicio incluido en la lista, por ejemplo, el certificado X.509v3 (como mínimo) de una CA que expide QC,

— para los servicios CA/QC, información opcional «Service information extensions» («Sie») que permitirá la inclusión de una secuencia de una o más tuplas, cada una de las cuales contiene:

  — los criterios que se utilizarán para precisar (filtrar) dentro del servicio de certificación identificado en el «Sdi» el servicio concreto (es decir, el conjunto de certificados reconocidos) para el que se exige/facilita información adicional con respecto a la indicación del respaldo por SSCD (o expedición a una persona jurídica), y

  — la información asociada («qualifiers») sobre si el conjunto de certificados reconocidos de este servicio precisado está o no respaldado por un SSCD o si esta información asociada forma parte del QC en una forma normalizada y procesable por una máquina, o información relativa al hecho de que tales QC se expiden a personas jurídicas (por defecto deben considerarse expedidas solamente a personas físicas),

▼C1

— información sobre el «estado actual» de esta entrada de servicio, indicando en particular:

— si se trata de un servicio supervisado o acreditado, y

— el estado de supervisión/acreditación propiamente dicho.

2.3. *Directrices de edición y uso de las entradas de servicios CSP_{QC}*

Las directrices generales de edición son:

1. Si se garantiza [garantía aportada por el CSP_{QC} y supervisada/acreditada por el organismo de supervisión (*Supervisory Body* o SB) o el organismo de acreditación (*Accreditation Body* o AB)] que, para un servicio de la lista identificado por una «Sdi», cualquier QC respaldado por un SSCD contiene la declaración QcCompliance definida por el ETSI y contiene la declaración QcSSCD o el identificador de objeto (OID) QCP+, entonces es suficiente el uso de una «Sdi» apropiada y puede utilizarse el campo «Sie» como opción sin que necesite contener la información sobre respaldo por SSCD.

2. Si se garantiza (garantía aportada por el CSP_{QC} y supervisada/acreditada por el SB/AB) que, para un servicio de la lista identificado por una «Sdi», cualquier QC no respaldado por un SSCD contiene la declaración QcCompliance o el OID QCP, y es tal que está pensado para no contener la declaración QcSSCD o el OID QCP+, entonces es suficiente el uso de una «Sdi» apropiada y puede utilizarse el campo «Sie» como opción sin que necesite contener la información sobre respaldo por SSCD (lo que significa que no está respaldado por un SSCD).

3. Si se garantiza (garantía aportada por el CSPQC y supervisada/acreditada por el SB/AB) que, para un servicio de la lista identificado por una «Sdi», ningún QC contiene la declaración QcCompliance, y algunos de estos QC están pensados para estar respaldados por SSCD y otros no (pudiendo, por ejemplo, diferenciarse por distintos OID de política de certificados específicos del CSP o por otra información específica del CSP en el QC, directa o indirectamente, procesable por una máquina o no), pero no contiene NI la declaración QcSSCD NI el OID QCP(+) del ETSI, entonces el uso de una «Sdi» apropiada podría no ser suficiente Y deberá usarse el campo «Sie» para consignar información explícita sobre el respaldo por SSCD junto con una potencial extensión de información para identificar el conjunto de certificados cubierto. Es probable que ello exija la inclusión de «SSCD support information values» diferentes para la misma «Sdi» cuando se haga uso del campo «Sie».

4. Si se garantiza (garantía aportada por el CSP_{QC} y supervisada/acreditada por el SB/AB) que, para un servicio de la lista identificado por una «Sdi», ningún QC contiene ni la declaración QcCompliance, ni el OID QCP, ni la declaración QcSSCD, ni el OID QCP+, pero se garantiza que algunos de estos certificados de entidad final expedidos bajo esta «Sdi» están pensados para constituir QC o respaldados por SSCD y otros no (pudiendo, por ejemplo, diferenciarse por distintos OID de política de certificados específicos del CSP o por otra información específica del CSP en el QC, directa o indirectamente, procesable por una máquina o no), entonces el uso de una «Sdi» apropiada no será suficiente Y deberá utilizarse el campo «Sie» para consignar información explícita sobre el respaldo por SSCD. Es probable que ello exija la inclusión de «SSCD support information values» diferentes para la misma «Sdi» cuando se haga uso del campo «Sie».

▼C1

Como principio general por defecto, para un CSP que figure en la lista de confianza deberá haber una entrada de servicio por cada certificado X.509v3 para un servicio de certificación de tipo CA/QC, es decir, una autoridad de certificación que expida (directamente) QC. En determinadas circunstancias cuidadosamente previstas y en condiciones cuidadosamente gestionadas, un organismo de supervisión o de acreditación de un Estado miembro podrá decidir utilizar el certificado X.509v3 de una CA raíz o de nivel superior (es decir, una autoridad de certificación que no expida directamente QC de entidad final, pero certifique una jerarquía de CA que descienda hasta las CA que expiden QC a entidades finales) como «Sdi» de una entrada determinada de la lista de servicios de un CSP que figure en la lista. Las consecuencias (ventajas y desventajas) de utilizar tal X.509v3 de una CA raíz o CA de nivel superior como valor «Sdi» de entradas de servicios de la TL deberá ser cuidadosamente estudiada y aprobada por los Estados miembros. Además, cuando se recurra a esta excepción autorizada al principio por defecto, el Estado miembro deberá aportar la documentación necesaria para facilitar la construcción y verificación de la trayectoria de certificación.

Presentamos el siguiente ejemplo para ilustrar las directrices generales sobre edición: En el contexto de un CSP_{QC} que utiliza una CA raíz bajo la cual varias CA expiden QC y no QC, pero cuyos QC contienen solo la declaración QcCompliance y ninguna indicación de si está respaldado por un SSCD, la inclusión en la lista del «Sdi» de la CA raíz significaría solamente, con arreglo a las reglas antes explicadas, que NINGÚN QC expedido bajo esta jerarquía de CA raíz está respaldado por un SSCD. Si estos QC están realmente respaldados por un SSCD, se recomendaría vivamente hacer uso de la declaración QcSSCD en los QC expedidos en el futuro. Mientras tanto (hasta que haya expirado el último QC que no contenga esta información), la TSL debería hacer uso del campo «Sie» y la extensión «Qualifications» asociada, por ejemplo, filtrando certificados a través de OID definidos por el CSPQC específicos utilizados potencialmente por el CSPQC para distinguir distintos tipos de QC (unos respaldados por un SSCD y otros no) e incluir una «SSCD support information» explícita con relación a estos certificados filtrados mediante el uso de «Qualifiers».

Las directrices generales de uso para las aplicaciones, servicios o productos de firma electrónica que se basan en una implementación TSL de una lista de confianza con arreglo a las presentes especificaciones técnicas son las siguientes:

Una entrada «Sti»«CA/QC» (y análogamente una entrada CA/QC que luego se precisa como «CA/QC raíz» mediante el uso de la extensión additionalServiceInformation en «Sie»)

— indica que a partir de la CA identificada en la «Sdi» (y análogamente dentro de la jerarquía de CA que comienza en la CA raíz identificada en la «Sdi»), todos los certificados de entidad final expedidos son QC siempre que así se consigne en el certificado mediante el uso de QcStatements apropiadas (es decir, QcC, QcSSCD) o OID QCP(+) definidos por el ETSI (y esto lo garantiza el organismo de supervisión/acreditación, véanse las precedentes «directrices generales de edición»).

Nota: Si no hay presente información «Qualification» de «Sie» o si un certificado de entidad final del que se afirma es un QC no se «precisa» mediante una entrada «Sie» relacionada, entonces la exactitud de la información «procesable por máquina» que se encuentra en el QC está supervisada/acreditada. Esto significa que está garantizado que el uso (o no uso) de las QcStatements adecuadas (es decir, QcC, QcSSCD) o OID QCP(+) definidos por el ETSI es conforme con lo que afirma el CSP_{QC},

▼C1

— y SI hay presente información «Qualification» de «Sie», entonces además de la regla de interpretación de uso por defecto precedente, los certificados que se identifican mediante el uso de esta entrada «Qualification» de «Sie», que se construye con arreglo al principio de una secuencia de «filtros» que precisa un conjunto de certificados y facilita alguna información adicional sobre el «respaldo por SSCD» o «persona jurídica como sujeto» (por ejemplo, los certificados que contienen un OID específico en la extensión de política de certificado o tienen un patrón específico de «Key usage» o filtrados mediante el uso de un valor específico que aparece en un campo específico o extensión del certificado, etc.), deben considerarse con arreglo al siguiente conjunto de «qualifiers», que compensan la ausencia de información en el QC correspondiente, a saber:

— para indicar respaldo por un SSCD:

  — el valor «QCWithSSCD» significa «QC respaldado por un SSCD», o

  — el valor «QCNoSSCD» significa «QC no respaldado por un SSCD», o

  — el valor «QCSSCDStatusAsInCert» significa que se garantiza que la información sobre respaldo por un SSCD está contenida en cualquier QC en la información facilitada en la «Sdi»-«Sie» en esta entrada CA/QC,

  O

— para indicar expedición a persona jurídica:

  — el valor «QCForLegalPerson» significa «Certificado expedido a una persona jurídica».

2.4. *Servicios que soportan servicios «CA/QC» pero no forman parte de la «Sdi» del «CA/QC»*

Es preciso también cubrir los casos en los que las CRL y las respuestas OCSP están firmadas por claves que no proceden de una CA que expide QC («CA/QC»). Esto puede conseguirse incluyendo estos servicios como tales en la implementación TSL de la TL (es decir, con un «Service type identifier» precisado mediante una extensión «additionalServiceInformation» que refleje que una OCSP o un servicio CRL forman parte de la prestación de QC, por ejemplo, con un tipo de servicio de «OCSP/QC» o «CRL/QC» respectivamente), ya que estos servicios pueden considerarse parte de los servicios «reconocidos» supervisados/acreditados relacionados con la prestación de los servicios de certificación de QC. Por supuesto, los respondedores de OCSP o los expedidores de CRL cuyos certificados estén firmados por CA bajo la jerarquía de un servicio CA/QC que figure en la lista deben considerarse «válidos» y conformes con el valor de estado del servicio CA/QC de la lista.

Similar disposición puede aplicarse a los servicios de certificación que expidan certificados no reconocidos (de un tipo de servicio «CA/PKC») utilizando los tipos de servicio OCSP y CRL por defecto de ETSI TS 102 231.

Nótese que la implementación TSL de la TL DEBERÁ incluir servicios de supresión cuando no conste información relacionada en el campo AIA de los certificados finales, o cuando no esté firmada por una CA que sea de las que figuran en la lista.

2.5. *Hacia un perfil QC interoperable*

Por norma general, deberá intentarse simplificar (reducir) en la mayor medida posible el número de entradas de servicios («Sdi» distintos). No obstante, habrá que conseguir un equilibrio entre esta intención y la correcta identificación de los servicios relacionados con la expedición de QC y el suministro de información de confianza sobre si estos QC están o no respaldados por un SSCD cuando falte esta información en el QC expedido.

▼C1

Idealmente, el uso del campo «Sie» y la extensión «Qualification» debería limitarse (estrictamente) a los casos concretos que deban resolverse así, ya que los QC deberían contener información suficiente en relación con el estado reconocido declarado y con el respaldo o no por un SSCD declarado.

Los Estados miembros deberían, en la mayor medida posible, fomentar la adopción y el uso de perfiles QC interoperables.

3. **Estructura del modelo común de la Lista de Confianza**

El modelo común propuesto para la lista de confianza de un Estado miembro se estructurará con arreglo a las siguientes categorías de información:

1. Información sobre la lista de confianza y su régimen de expedición.

2. Una secuencia de campos que contenga información de identificación no ambigua sobre cada uno de los CSP supervisados/acreditados en virtud del régimen (esta secuencia es opcional, es decir, si no se usa se considerará la lista vacía, lo que significará que no hay ningún CSP supervisado o acreditado en el Estado miembro correspondiente en el contexto del ámbito de la lista de confianza).

3. Para cada CSP de la lista, una secuencia de campos que contenga una identificación no ambigua de un servicio de certificación supervisado/acreditado prestado por el CSP (esta secuencia deberá tener como mínimo una entrada),

4. Para cada servicio de certificación supervisado/acreditado de la lista, identificación del estado actual del servicio e historia de dicho estado.

En el contexto de un CSP que expide QC, la identificación no ambigua de un servicio de certificación supervisado/acreditado de la lista deberá tomar en consideración las situaciones en que no se dispone de información suficiente en el certificado reconocido sobre su estado «reconocido», su respaldo potencial por un SSCD y especialmente el hecho adicional de que la mayoría de los CSP (comerciales) utilizan una única CA reconocida para expedir varios tipos de certificados de entidad final, tanto reconocidos como no reconocidos.

El número de entradas de la lista por CSP reconocido podría reducirse si existen uno o varios servicios CA de nivel superior, por ejemplo, en el contexto de una jerarquía comercial de CA que descienda desde una CA raíz a las CA expedidoras. No obstante, incluso en estos casos, tendrá que mantenerse y garantizarse el principio de que exista un vínculo no ambiguo entre un servicio de certificación CSP_{QC} y el conjunto de certificados que se desea se identifiquen como QC.

1. *Información sobre la lista de confianza y su régimen de expedición*

Formará parte de esta categoría la información siguiente:

— Una etiqueta de lista de confianza que facilite la identificación de la lista de confianza en las búsquedas electrónicas y también confirme sus propósitos cuando esté en forma legible por las personas.

— Un identificador de formato y versión del formato de la lista de confianza.

— Un número de secuencia (o de versión) de la lista de confianza.

— Una información sobre el tipo de lista de confianza (por ejemplo, para indicar que esta lista de confianza facilita información sobre el estado de supervisión/acreditación de los servicios de certificación prestados por CSP supervisados/acreditados por el Estado miembro de referencia en cuanto al cumplimiento de lo dispuesto en la Directiva 1999/93/CE).

▼C1

— Una información sobre el propietario de la lista de confianza (por ejemplo, nombre, dirección, información de contacto, etc. del organismo del Estado miembro encargado de establecer, publicar de forma segura y mantener la lista de confianza).

— Información sobre el régimen o los regímenes de supervisión/acreditación subyacentes a los que está asociada la lista de confianza, incluyendo, sin limitarse a ello:

  — el país en que se aplica,

  — información sobre dónde se puede encontrar información sobre el régimen o los regímenes o referencia a ella (modelo de régimen, reglas, criterios, comunidad aplicable, tipo, etc.),

  — período de conservación de la información (histórica).

— Política o aviso legal y responsabilidades de la lista de confianza.

— Fecha y lugar de expedición y próxima actualización prevista de la lista de confianza.

2. *Información de identificación no ambigua sobre cada CSP reconocido por el régimen*

Este conjunto de información incluirá al menos lo siguiente:

— el nombre de la organización CSP tal como se utiliza en los registros legales oficiales (esto podrá incluir el UID de la organización CSP según las prácticas del Estado miembro),

— la dirección e información de contacto del CSP,

— información adicional sobre el CSP, bien incluida directamente, bien indicando algún lugar del que pueda descargarse tal información.

3. *Para cada CSP de la lista, una secuencia de campos que contengan una identificación no ambigua de un servicio de certificación prestado por el CSP y supervisado/acreditado en el contexto de la Directiva 1999/93/CE*

Este conjunto de información incluirá al menos lo siguiente para cada servicio de certificación de un CSP de la lista:

— un identificador del tipo de servicio de certificación (por ejemplo, identificador que indique que el servicio de certificación supervisado/acreditado del CSP es una autoridad de certificación que expide QC),

— nombre (comercial) de este servicio de certificación,

— un identificador único y no ambiguo del servicio de certificación,

— información adicional sobre el servicio de certificación (por ejemplo, incluida directamente o indicando algún lugar del que pueda descargarse tal información, información de acceso en relación con el servicio),

— para los servicios CA/QC, una secuencia opcional de tuplas de información, en la que cada tupla contiene:

  i) los criterios que deben utilizarse para precisar (filtrar) dentro del servicio de certificación identificado en el «Sdi» el servicio concreto (es decir, el conjunto de certificados reconocidos) para el que se exige/facilita información adicional con respecto a la indicación del respaldo por SSCD (o expedición a una persona jurídica), y

  ii) los «qualifiers» asociados que faciliten información sobre si el conjunto de certificados reconocidos de este servicio precisado está respaldado por un SSCD o no, o información sobre si tales QC se expiden a una persona jurídica (por defecto deben considerarse expedidos a personas físicas).

▼C1

4. *Para cada servicio de certificación de la lista, la identificación del estado actual del servicio y la historia de este estado.*

Este conjunto de información incluirá al menos lo siguiente:

— un identificador del estado actual,

— fecha y hora de inicio del estado actual,

— información histórica sobre este estado.

4. **Definiciones y abreviaturas**

A efectos del presente documento, se aplicarán las siguientes definiciones y acrónimos:

Término	Acrónimo	Definición
Proveedor de servicios de certificación	CSP	Según se define en el artículo 2, punto 11, de la Directiva 1999/93/CE.
Autoridad de certificación	CA	Una CA es un CSP y puede usar varias claves técnicas de firma privadas de la CA, cada una con un certificado asociado, a fin de expedir certificados de entidad final. Una CA es una autoridad en la que confían uno o más usuarios para la creación y asignación de certificados. Opcionalmente, la autoridad de certificación puede crear las claves de los usuarios [ETSI TS 102 042]. Se considera que la CA queda identificada por la información de identificación presente en el campo Issuer del certificado de CA relacionado con (que certifica) la clave pública asociada con la clave de firma privada de la CA y que, efectivamente, utiliza la CA para expedir certificados de entidad. Una CA puede tener varias claves de firma, cada una de ellas identificada de manera inequívoca por un identificador único dentro del campo Authority Key Identifier del certificado de la CA.
Autoridad de certificación que expide certificados reconocidos	CA/QC	Una CA que cumple los requisitos establecidos en el anexo II de la Directiva 1999/93/CE y expide certificados reconocidos que cumplen los requisitos establecidos en el anexo I de la Directiva 1999/93/CE.
Certificado	Certificado	Según se define en el artículo 2, punto 9, de la Directiva 1999/93/CE.
Certificado reconocido	QC	Según se define en el artículo 2, punto 10, de la Directiva 1999/93/CE.
Firmante	Firmante	Según se define en el artículo 2, punto 3, de la Directiva 1999/93/CE.
Supervisión	Supervisión	Se utiliza en el sentido de la Directiva 1999/93/CE (artículo 3, apartado 3). La Directiva exige a los Estados miembros que establezcan un sistema adecuado que permita la supervisión de los CSP establecidos en su territorio que expiden al público certificados reconocidos, garantizando la supervisión del cumplimiento de lo dispuesto en la Directiva.
Acreditación voluntaria	Acreditación	Según se define en el artículo 2, punto 13, de la Directiva 1999/93/CE.
Lista de confianza	TL	Designa la lista que indica el estado de supervisión/acreditación de los servicios de certificación de los proveedores de servicios de certificación que están supervisados/acreditados por el Estado miembro de referencia en cuanto al cumplimiento de lo dispuesto en la Directiva 1999/93/CE.

▼C1

Término	Acrónimo	Definición
Lista de estado de los servicios de confianza	TSL	Forma de una lista firmada que se utiliza como base para la presentación de información sobre el estado de los servicios de confianza con arreglo a las especificaciones contenidas en ETSI TS 102 231.
Servicio de confianza		Servicio que potencia la confianza en las transacciones electrónicas (habitualmente, pero no siempre, usando técnicas criptográficas o mediante material confidencial) (ETSI TS 102 231).
Proveedor de servicios de confianza	TSP	Organismo que gestiona uno o más servicios de confianza (electrónicos). El término se utiliza en un sentido más amplio que el de CSP.
Token de servicio de confianza	TrST	Objeto físico o binario (lógico) generado o expedido de resultas del uso de un servicio de confianza. Ejemplos de TrST binarios son los certificados, CRL, sellos temporales y respuestas OCSP.
Firma electrónica reconocida	QES	Una AdES respaldada por un QC y que se crea mediante un SSCD según se define en el artículo 2 de la Directiva 1999/93/CE.
Firma electrónica avanzada	AdES	Según se define en el artículo 2, punto 2, de la Directiva 1999/93/CE.
Firma electrónica avanzada respaldada por un certificado reconocido	$AdES_{QC}$	Una firma electrónica que cumple los requisitos de un AdES y está respaldada por un QC según se define en el artículo 2 de la Directiva 1999/93/CE.
Dispositivo seguro de creación de firma	SSCD	Según se define en el artículo 2, punto 6, de la Directiva 1999/93/CE.

CAPÍTULO I

ESPECIFICACIONES DETALLADAS PARA EL MODELO COMÚN DE LA «LISTA DE CONFIANZA DE PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN SUPERVISADOS/ACREDITADOS»

En la siguiente parte del documento, las palabras clave «DEBERÁ» (MUST), «NO DEBERÁ» (MUST NOT), «OBLIGATORIO» (REQUIRED), el «tiempo futuro» (SHALL), el «tiempo futuro negativo» (SHALL NOT), «DEBERÍA» (SHOULD), «NO DEBERÍA» (SHOULD NOT), «RECOMENDADO» (RECOMMENDED), «PODRÁ» (MAY), y «OPCIONAL» (OPTIONAL), o sus variantes gramaticales, deberán interpretarse de acuerdo con lo descrito para sus equivalentes en lengua inglesa en el documento RFC 2119 ([1]).

►**M1** Las presentes especificaciones se basan en las especificaciones y requisitos contenidos en la norma ETSI TS 102 231 v3.1.2. Cuando en las presentes especificaciones no se establezca ningún requisito específico, SE APLICARÁN íntegramente los requisitos de ETSI TS 102 231 v.3.1.2. ◄ Cuando figuren requisitos específicos, estos PREVALECERÁN sobre los requisitos correspondientes de ETSI TS 102 231, completados por las especificaciones de formato contenidas en ETSI TS 102 231. En caso de discrepancia entre las presentes especificaciones y las especificaciones de ETSI TS 102 231, las primeras SERÁN las normativas.

([1]) IETF RFC 2119: «Key words for use in RFCs to indicate Requirements Levels».

▼C1

SE IMPLEMENTARÁ el soporte de lenguas y se facilitará al menos en inglés (EN) y además, potencialmente, en una o más lenguas nacionales.

La indicación de fecha y hora SE AJUSTARÁ a la cláusula 5.1.4 de ETSI TS 102 231.

El uso de URI SE AJUSTARÁ a la cláusula 5.1.5 de ETSI TS 102 231.

Información sobre el régimen de expedición de la lista de confianza

Tag

TSL tag (cláusula 5.2.1)

Este campo es OBLIGATORIO y SE AJUSTARÁ a la cláusula 5.2.1 de ETSI TS 102 231.

▼M1

_____

▼C1

Scheme Information

TSL version identifier (cláusula 5.3.1)

Este campo es OBLIGATORIO y su valor DEBERÁ ser «3» (entero).

TSL sequence number (cláusula 5.3.2)

▼M1

Este campo es OBLIGATORIO y ESPECIFICARÁ el número de secuencia del TSL. Este valor entero, que será «1» en la primera versión de la TSL, SE INCREMENTARÁ a cada versión posterior de la misma. NO SE REINICIARÁ a «1» cuando se incremente el valor del «TSL version identifier».

▼C1

TSL type (cláusula 5.3.3)

▼M1

Este campo es OBLIGATORIO y especifica el tipo de TSL. Su valor SE PONDRÁ a http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/-generic (genérico).

▼C1

Nota: A fin de ajustarse a ETSI TS 102 231, cláusula 5.3.3, e indicar el tipo específico de TSL mientras se hace referencia a la existencia de las presentes especificaciones que rigen el establecimiento de la implementaciónTSL de la lista de confianza de los Estados miembros ([1]) y permitir que un analizador sintáctico determine qué forma de cualquiera de los campos siguientes ([2]) debe esperar, cuando estos campos tengan significados específicos (o alternativos) con arreglo al tipo de TSL representado (en este caso constituir la lista de confianza de un Estado miembro), el URI específico SE REGISTRARÁ y DESCRIBIRÁ de la siguiente manera:

([1]) Es decir, la «Lista del estado de supervisión/acreditación de los servicios de certificación de los proveedores de servicios de certificación que están supervisados/acreditados por el Estado miembro de referencia en cuanto al cumplimiento de lo dispuesto en la Directiva 1999/93/CE» (abreviadamente, «la lista de confianza»).

([2]) Los campos especificados por ETSI TS 102 231 — *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information* y «perfilados» por las presentes especificaciones para especificar el establecimiento de la lista de confianza de los Estados miembros.

▼M1

URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic

▼C1

Descripción: Una implementación TSL de una lista que indica el estado de supervisión/acreditación de los servicios de certificación de los proveedores de servicios de certificación que están supervisados/acreditados por el Estado miembro de referencia poseedor de la implementación TSL en cuanto al cumplimiento de las disposiciones pertinentes establecidas en la Directiva 1999/93/CE, mediante un proceso de vigilancia directa (sea voluntaria o por ley).

Scheme operator name (cláusula 5.3.4)

Este campo es OBLIGATORIO. ESPECIFICARÁ el nombre del organismo del Estado miembro encargado de establecer, publicar y mantener la lista de confianza nacional. ESPECIFICARÁ la denominación oficial con la que opera la entidad jurídica o la entidad mandataria (por ejemplo, para las agencias administrativas públicas) asociada a este organismo. DEBERÁ ser la denominación utilizada en el registro o autorización legal oficial y a la cual deben dirigirse las comunicaciones oficiales. DEBERÁ ser una secuencia de cadenas de caracteres multilingües y DEBERÁ implementarse con el inglés (EN) como lengua obligatoria y con, potencialmente, una o más lenguas nacionales.

Nota: Un país PODRÁ tener organismos de supervisión y acreditación distintos e incluso organismos adicionales para las eventuales actividades operativas conexas. ►M1 Compete a cada Estado miembro designar al operador del régimen de implementación TSL de la TL del Estado miembro. ◄ Se espera que el organismo de supervisión, el organismo de acreditación y el operador del régimen (cuando se trate de organismos distintos) tengan cada uno sus propias responsabilidades.

Cualquier situación en la que sean varios los organismos responsables de la supervisión, la acreditación o los aspectos operativos DEBERÁ reflejarse de manera coherente e identificarse como tal en la información sobre el régimen que figura en la TL, incluida la información específica del régimen indicada por el «Scheme information URI» (cláusula 5.3.7).

▼M1

El operador del régimen designado (cláusula 5.3.4) será la entidad que firme la TSL.

▼C1

Scheme operator address (cláusula 5.3.5)

Este campo es OBLIGATORIO. ESPECIFICARÁ la dirección de la entidad jurídica u organización mandatria identificada en el campo «Scheme operator name» (cláusula 5.3.4) para comunicaciones tanto postales como electrónicas. INCLUIRÁ tanto la «PostalAddress» (es decir, calle, localidad, [estado o provincia], [código postal] y código de país ISO 3166-1 alfa-2) con arreglo a la cláusula 5.3.5.1; como la «ElectronicAddress» (es decir, correo electrónico o URI del sitio web) con arreglo a la cláusula 5.3.5.2.

Scheme name (cláusula 5.3.6)

Este campo es OBLIGATORIO y especificará la denominación bajo la que actúa el régimen. SERÁ una secuencia de cadenas de caracteres multilingües (con EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales) definida así:

▼C1

— La versión EN SERÁ una cadena de caracteres estructurada como sigue:

CC:EN_name_value

donde:

— «CC» = el código de país ISO 3166-1 alfa-2 utilizado en el campo «Scheme territory» (cláusula 5.3.10),

— «:» = se utiliza como separador,

▼M1

— «EN_name_value» = Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State's laws.

▼C1

— Las eventuales versiones en las lenguas nacionales del Estado miembro SERÁN una cadena de caracteres estructurada como sigue:

CC:name_value

donde:

— «CC» = el código de país ISO 3166-1 alfa-2 utilizado en el campo «Scheme territory» (cláusula 5.3.10),

— «:» = se utiliza como separador,

— «name_value» = traducción oficial a la lengua nacional del anterior «EN_name_value».

La denominación del régimen debe identificar de manera única, por su nombre, al régimen a que se hace referencia mediante el «Scheme information URI», y también garantizar que, en caso de que el operador de un régimen opere más de uno, cada uno de ellos tenga una denominación distinta.

Los Estados miembros y los operadores de regímenes SE ASEGURARÁN de que cuando un Estado miembro o un operador de régimen operen más de un régimen, cada uno de ellos reciba una denominación distinta.

Scheme information URI (cláusula 5.3.7)

Este campo es OBLIGATORIO y ESPECIFICARÁ el URI o los URI en los que las partes usuarias pueden obtener información específica del régimen (con el EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales). Esta SERÁ una secuencia de indicadores multilingües (con el EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales). La URI o las URI especificadas DEBERÁN facilitar un camino hacia la información que constituya la «información apropiada sobre el régimen».

La «información apropiada sobre el régimen» INCLUIRÁ como mínimo:

— Información general introductoria que sería común a todos los Estados miembros con respecto al alcance y al contexto de la lista de confianza, y los regímenes de supervisión/acreditación subyacentes. El texto común que se utilizará es el siguiente:

▼C1

«The present list is the TSL implementation of [name of the relevant Member State] "Trusted List of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [name of the relevant Member State] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable "supervision" system (respectively "voluntary accreditation" system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art. 2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.»

— Información específica sobre el régimen o los regímenes de supervisión/-acreditación subyacentes, en particular [1]:

— información sobre el sistema de supervisión aplicable a cualquier CSP_{QC},

[1] Los dos últimos conjuntos de información son de importancia crítica para que las partes usuarias evalúen el nivel de calidad y seguridad de tales sistemas de supervisión/-acreditación. Estos conjuntos de información se facilitarán a nivel de la TL 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 que remite a la Directiva 1999/93/CE, junto con la posibilidad de que cada Estado miembro añada textos/referencias específicas del mismo). Podrá facilitarse información adicional sobre los sistemas nacionales de supervisión/acreditación para los CSP que no expidan QC a nivel de servicio si procede y resulta necesario (por ejemplo, para distinguir entre varios niveles de calidad/seguridad) mediante el uso del «Scheme service definition URI» (cláusula 5.5.6).

▼C1

— información, cuando proceda, sobre el régimen nacional de acreditación voluntaria aplicable a cualquier CSP_{QC},

— información, cuando proceda, sobre el sistema de supervisión aplicable a cualquier CSP que no expida QC,

— información, cuando proceda, sobre el régimen nacional de acreditación voluntaria aplicable a cualquier CSP que no expida QC.

— Esta información específica INCLUIRÁ, como mínimo, para cada régimen subyacente enumerado:

— una descripción general,

— información sobre el proceso seguido por el organismo de supervisión/acreditación para supervisar/acreditar a los CSP y por los CSP para ser supervisados/acreditados,

— información sobre los criterios con arreglo a los cuales se supervisan/acreditan los CSP.

— Información específica, cuando proceda, sobre los «reconocimientos» específicos que algunos de los objetos físicos o binarios (lógicos) generados o expedidos de resultas de la prestación de un servicio de certificación pueden recibir por ajustarse a las disposiciones y requisitos establecidos a nivel nacional, incluido el significado de tal «reconocimiento» y las disposiciones y requisitos nacionales asociados.

Además, PODRÁ facilitarse con carácter voluntario información adicional específica del Estado miembro sobre el régimen. Esta INCLUIRÁ:

— información sobre los criterios y reglas utilizados para seleccionar a los supervisores/auditores y definir cómo supervisan (controlan)/acreditan (auditan) estos a los CSP,

— otra información de contacto y general aplicable al funcionamiento del régimen.

Status determination approach (cláusula 5.3.8)

Este campo es OBLIGATORIO y ESPECIFICARÁ el identificador del método de determinación del estado. SE UTILIZARÁ el siguiente URI específico, según se registra y describe a continuación:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate

Descripción: El estado de los servicios de la lista lo determina el operador del régimen (o se determina en su nombre) con arreglo a un sistema apropiado para un Estado miembro de referencia que permita la «supervisión» (y, si procede, «acreditación voluntaria») de los proveedores de servicios de certificación establecidos en su territorio (o establecidos en un tercer país en el caso de la «acreditación voluntaria») y expida certificados reconocidos al público con arreglo al artículo 3, apartado 3 [respectivamente artículo 3, apartado 2 o artículo 7, apartado 1, letra a)] de la Directiva 1999/93/CE, y, si procede, que permita la «supervisión»/«acreditación voluntaria» de los proveedores de servicios de certificación que no expidan certificados reconocidos, con arreglo a uno o más «regímenes de aprobación reconocidos» definidos y establecidos a nivel nacional e implementados a ese mismo nivel para la supervisión del cumplimiento por los servicios de los CSP que no expiden QC de las disposiciones establecidas en la Directiva 1999/93/CE y potencialmente ampliadas por disposiciones nacionales con respecto a la prestación de tales servicios de certificación.

▼C1

Scheme type/community/rules (cláusula 5.3.9)

Este campo es OBLIGATORIO y CONTENDRÁ al menos los siguientes URI registrados:

— Un URI común a todas las listas de confianza de los Estado miembros que lleve a un texto descriptivo que SERÁ aplicable a todas las TL:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— mediante el cual se denota la participación del régimen del Estado miembro (identificado a través del «TSL type» (cláusula 5.3.3) y «Scheme name» (cláusula 5.3.6) en un sistema de regímenes (es decir, una TSL que contiene indicadores a todos los Estado miembros que publican y mantienen una TL en forma de TSL);

— en el que los usuarios pueden obtener la política o las reglas con arreglo a las cuales SE EVALUARÁN los servicios incluidos en la lista y que permitan determinar el tipo de TSL (véase la cláusula 5.3.3),

— en el que los usuarios pueden obtener una descripción sobre cómo usar e interpretar el contenido de la implementación TSL de la Lista de Confianza; estas reglas de uso SERÁN comunes a todas las listas de confianza de los Estados miembros sea cual sea el tipo de servicio que figure en la lista y sean cuales sean los sistemas de supervisión/acreditación.

Texto descriptivo:

«Participation in a scheme

Each Member State must create a "Trusted List of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

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

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C1

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable "supervision" system (respectively "voluntary accreditation" system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art. 2.13, Art. 3.2, Art. 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a "voluntary accreditation" system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined "recognised approval scheme" implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2.11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific "qualification" on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a "qualification" is likely to be limited solely to the national level.

Interpretation of the TSL implementation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EC are as follows:

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

— indicates that from the "Service digital identifier" ("Sdi") identified CA (similarly within the CA hierarchy starting from the "Sdi" identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) provided that it is claimed as such in the certificate through the use of appropriate ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

Note: if no “Sie”“Qualification” information is present or if an end-entity certificate that is claimed to be a QC is not “further identified” through a related “Sie” entry, then the “machine-processable” information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— and IF “Sie”“Qualification” information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this “Sie”“Qualification” entry, which is constructed on the principle of a sequence of “filters” further identifying a set of certificates, must be considered according to the associated “qualifiers” providing some additional information regarding “SSCD support” and/or “Legal person as subject” (e.g. those 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.). Those qualifiers are part of the following set of “qualifiers” used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

  — to indicate the nature of the SSCD support:

    — “QCWithSSCD” qualifier value meaning “QC supported by an SSCD”, or

    — “QCNoSSCD” qualifier value meaning “QC not supported by an SSCD”, or

    — “QCSSCDStatusAsInCert” qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the “Sdi”-“Sie” provided information in this CA/QC entry;

  AND/OR

  — to indicate issuance to Legal Person:

    — “QCForLegalPerson” qualifier value meaning “Certificate issued to a Legal Person”

The general interpretation rule for any other “Sti” type entry is that the listed service named according to the “Sn” field value and uniquely identified by the “Sdi” field value has a current supervision/accreditation status according to the “Scs” 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 Technical specifications for a Common Template for the “Trusted List of supervised/accredited Certification Service Providers” in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the TSL implementation of the Member States’ Trusted Lists.»

▼C1

— Un URI específico de la Lista de Confianza del Estado miembro que lleve a un texto descriptivo que SERÁ aplicable a la TL de este Estado miembro:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

donde CC = el código de país ISO 3166-1 alfa-2 utilizado en el campo "Scheme territory" (cláusula 5.3.10).

— en el que los usuarios pueden obtener la política o las reglas específicas del Estado miembro de referencia con arreglo a las que SE EVALUARÁN los servicios incluidos en la lista en cumplimiento del sistema de supervisión y los regímenes de acreditación voluntaria apropiados del Estado miembro,

— en el que los usuarios pueden obtener una descripción específica del Estado miembro de referencia sobre cómo usar e interpretar el contenido de la implementación TSL de la Lista de Confianza con respecto a los servicios de certificación no relacionados con la expedición de QC; esto podrá utilizarse para indicar una granularidad potencial en los sistemas de supervisión/acreditación nacionales 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».

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

Scheme territory (cláusula 5.3.10)

En el contexto de las presentes especificaciones, este campo es OBLIGATORIO y ESPECIFICARÁ el país en que está establecido el régimen (código de país ISO 3166-1 alfa-2).

TSL policy/legal notice (cláusula 5.3.11)

En el contexto de las presentes especificaciones, este campo es OBLIGATORIO y ESPECIFICARÁ la política del régimen o facilitará un anuncio sobre la situación jurídica del régimen o los requisitos legales que este satisface en la jurisdicción en la que está establecido o cualquier restricción o condición bajo la cual se mantenga y publique la TL.

SERÁ una cadena de caracteres multilingües (texto sencillo) compuesta por dos partes:

— Una primera parte obligatoria, común a todas las TL de los Estados miembros (con el EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales), que indique que el marco jurídico aplicable es la Directiva 1999/93/CE y la legislación que la incorpora al Derecho interno del Estado miembro indicado en el campo «Scheme Territory».

Texto común en lengua inglesa:

«The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.e»

Texto, en la lengua o las lenguas nacionales del Estado miembro, que sea traducción oficial del texto inglés precedente.

▼C1

— Una segunda parte opcional, específica de cada TL (con el EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales), que contenga referencias a los marcos jurídicos nacionales específicos aplicables (por ejemplo, en particular cuando se relacionan con regímenes de supervisión/-acreditación nacionales para CSP que no expiden QC).

Historical information period (cláusula 5.3.12)

Este campo es OBLIGATORIO y ESPECIFICARÁ el período (valor entero) para el que se facilita información histórica en la TSL. Este valor entero se dará en número de días y, en el contexto de las presentes especificaciones, SERÁ mayor o igual a 3 653 (es decir que la implementación TSL de la TL de los Estados miembros DEBERÁ contener información histórica sobre un mínimo de diez años). Los valores más grandes deberían tener debidamente en cuenta los requisitos legales de conservación de datos en el Estado miembro indicado en el «Scheme Territory» (cláusula 5.3.10).

Pointers to other TSLs (cláusula 5.3.13)

En el contexto de las presentes especificaciones, este campo es OBLIGATORIO e INCLUIRÁ, cuando se disponga de él, el indicador que apunte a una forma compatible con ETSI TS 102 231 de la lista compilada por la CE de enlaces (indicadores) hacia todas las implementaciones TSL de las listas de confianza de los Estados miembros. Se aplicarán las especificaciones de ETSI TS 102 231, cláusula 5.3.13, si se impone el uso de la identidad digital opcional, que representa el expedidor de la TSL indicada, formateada como se especifica en la cláusula 5.5.3.

Nota: A la espera de una implementación ajustada a ETSI TS 102 231 de la lista compilada por la CE de enlaces hacia la implementación TSL de las TL de los Estados miembros, NO SE UTILIZARÁ este campo.

List issue date and time (cláusula 5.3.14)

Este campo es OBLIGATORIO y ESPECIFICARÁ la fecha y la hora (UTC expresado como hora Z) en que se expidió la TSL utilizando el valor de fecha y hora según se especifica en ETSI TS 102 231, cláusula 5.1.4.

Next update (cláusula 5.3.15)

Este campo es OBLIGATORIO y ESPECIFICARÁ la fecha y la hora (UTC expresado como hora Z) límite para la expedición de la siguiente TSL o será nulo, lo que indicará TSL cerrada (utilizando el valor de fecha y hora según se especifica en ETSI TS 102 231, cláusula 5.1.4).

En caso de no haber cambios de estado intermedios para ningún TSP ni servicio cubierto por el régimen, la TSL DEBERÁ ser reexpedida antes de que expire la última TSL expedida.

En el contexto de las presentes especificaciones, la diferencia entra la fecha y hora de «Next update» y la «List issue date and time» NO EXCEDERÁ de seis (6) meses.

▼C1

Distribution points (cláusula 5.3.16)

Este campo es OPCIONAL. Si se usa, ESPECIFICARÁ los lugares en que está publicada la actual implementación TSL de la TL y en que se pueden encontrar las actualizaciones de la TSL actual. Si se especifican varios puntos de distribución, todos DEBERÁN ofrecer copias idénticas de la TSL actual o su versión actualizada. Cuando se utilice, su formato será una secuencia no vacía de cadenas, todas las cuales se ajustarán a RFC 3986 ([1]).

Scheme extensions (cláusula 5.3.17)

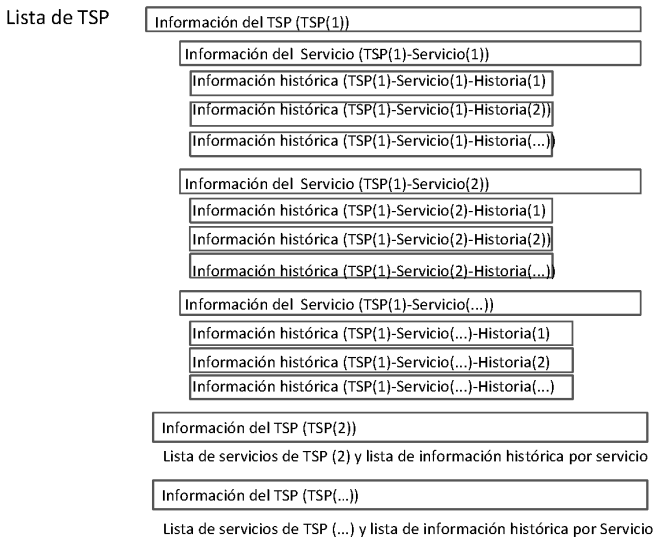
Este campo es OPCIONAL y no se usa en el contexto de la presente especificación.

List of Trust Service Providers

Este campo es OPCIONAL.

En caso de que no existan o hayan existido CSP supervisados/acreditados en el contexto del régimen en un Estado miembro, esté campo ESTARÁ ausente. Se conviene, no obstante, en que incluso si un Estado miembro no tiene ningún CSP supervisado o acreditado por el régimen, los Estados miembros IMPLEMENTARÁN una TSL con este campo ausente. La inexistencia de CSP en la lista SIGNIFICARÁ que no hay CSP que estén supervisados/acreditados en el país especificado en el «Scheme Territory».

En el caso de que haya o haya habido uno o más servicios de CSP supervisados/acreditados por el régimen, este campo CONTENDRÁ una secuencia que identifique cada CSP que preste uno o más de estos servicios supervisados/acreditados, con detalles sobre los estados de supervisión/-acreditación y su historia para cada uno de los servicios del CSP (TSP = CSP en la siguiente figura).



([1]) IETF RFC 3986: «Uniform Resource Identifiers (URI): Generic syntax».

▼C1

La lista de TSP se organiza según muestra la figura precedente. Para cada TSP, hay una secuencia de campos que contienen información sobre el TSP («TSP Information»), seguida de una lista de servicios. Para cada servicio de la lista, hay una secuencia de campos que contienen información sobre el servicio («Service Information») y una secuencia de campos sobre la historia del estado de aprobación del servicio («Service approval history»).

TSP Information

TSP(1)

TSP name (cláusula 5.4.1)

Este campo es OBLIGATORIO y ESPECIFICARÁ la denominación de la entidad jurídica responsable de los servicios del CSP que están supervisados o acreditados dentro del régimen o lo han estado. Se trata de una secuencia de cadenas de caracteres multilingües (con el EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales). Esta denominación DEBERÁ ser la utilizada en los registros legales oficiales y a la que se dirigiría cualquier comunicación oficial.

TSP trade name (cláusula 5.4.2)

Este campo es OPCIONAL y, si se utiliza, ESPECIFICARÁ una denominación alternativa con la que se identifique el CSP en el contexto específico de la prestación de aquellos de sus servicios que figuran en esta TSL bajo la entrada «TSP name» (cláusula 5.4.1).

Nota: Cuando un CSP que sea una única entidad jurídica preste servicios utilizando denominaciones comerciales diferentes o en contextos específicos diferentes, podría haber tantas entradas de CSP como contextos específicos (por ejemplo, entradas con denominación/denominación comercial). Una alternativa es poner en la lista una sola vez cada CSP (entidad jurídica) y presentar información sobre contextos específicos del servicio. Corresponde al operador del régimen del Estado miembro debatir y concertar con los CSP cuál es el enfoque más adecuado.

TSP address (cláusula 5.4.3)

Este campo es OBLIGATORIO y ESPECIFICARÁ la dirección de la entidad jurídica u organización mandataria identificada en el campo «TSP name» (cláusula 5.4.1) tanto para comunicaciones postales como electrónicas. INCLUIRÁ tanto la «PostalAddress» (es decir, calle, población, [estado o provincia], [código postal] y código de país ISO 3166-1 alfa-2) de acuerdo con la cláusula 5.3.5.1, como la «ElectronicAddress» (es decir, correo electrónico y/o sitio web URI) de acuerdo con la cláusula 5.3.5.2.

TSP information URI (cláusula 5.4.4)

Este campo es OBLIGATORIO y ESPECIFICARÁ el URI o los URI en las que las partes usuarias pueden obtener información específica sobre un CSP. CONSISTIRÁ en una secuencia de indicadores multilingües (con el EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales). El URI o los URI mencionados DEBERÁN llevar a una información que describa las condiciones generales del CSP, sus prácticas, aspectos jurídicos, políticas de atención al cliente y otra información genérica aplicable a todos sus servicios enumerados en la entrada del CSP de la TSL.

Nota: Cuando un CSP que es una única entidad jurídica presta servicios utilizando denominaciones comerciales diferentes o en contextos específicos diferentes, y ello se haya reflejado en tantas entradas de TSP como contextos específicos, este campo ESPECIFICARÁ información relacionada con el conjunto específico de servicios enumerados dentro de una entrada TSP/TradeName particular.

▼C1

TSP information extensions (cláusula 5.4.5)

Este campo es OPCIONAL y, si está presente, PODRÁ utilizarlo el operador del régimen, con arreglo a las especificaciones de ETSI TS 102 231 (cláusula 5.4.5), para facilitar información específica que se interpretará con arreglo a las reglas del régimen específico.

List of Services

Este campo es OBLIGATORIO y CONTENDRÁ una secuencia que identifique cada uno de los servicios reconocidos del CSP y el estado de aprobación (junto con la historia de dicho estado) de ese servicio. Deberá figurar en la lista al menos un servicio (incluso si la información es meramente histórica).

Dado que la conservación de información histórica sobre los servicios de la lista es OBLIGATORIA en virtud de las presentes especificaciones, esta información histórica DEBERÁ ser conservada incluso si el estado actual del servicio no exigiría normalmente que figurara en la lista (por ejemplo, el servicio ha sido suprimido). Así pues, DEBERÁ incluirse un CSP incluso si el único de sus servicios que figura en la lista se encuentra en tal estado, a fin de conservar la historia.

Service Information

TSP(1) Service(1)

Service type identifier (cláusula 5.5.1)

▼M1

Este campo es OBLIGATORIO y ESPECIFICARÁ el identificador del tipo de servicio con arreglo al tipo de las especificaciones de la presente TSL (es decir, «/eSigDir-1999-93-EC-TrustedList/TSLType/generic»).

▼C1

Cuando el servicio de la lista está relacionado con la expedición de certificados reconocidos, el URI citado SERÁ http://uri.etsi.org/TrstSvc/Svctype/CA/QC (una autoridad de certificación que expide certificados reconocidos).

Cuando el servicio de la lista está relacionado con la expedición de tokens de servicio de confianza que no sean QC y no admita la expedición de QC, el URI citado SERÁ uno de los URI definidos en ETSI 102 231 y enumerados en su cláusula D.2, adecuado para este campo. Esto SE APLICARÁ incluso para los tokens de servicio de confianza que estén supervisados/acreditados en cuanto al cumplimiento de algunas cualificaciones específicas con arreglo al Derecho interno de los Estados miembros (por ejemplo, el denominado token de sello temporal reconocido en DE o HU); el URI citado SERÁ uno de los URI definidos en ETSI 102 231 y enumerados en su cláusula D.2, adecuado para este campo (por ejemplo, TSA para los token de sello temporal reconocido definidos a nivel nacional). Cuando proceda, este reconocimiento nacional específico de los tokens de servicio de confianza PODRÁ figurar en la entrada del servicio, y SE UTILIZARÁ a tal efecto la extensión additionalServiceInformation (cláusula 5.8.2) de la cláusula 5.5.9 («Service information extension»).

▼C1

Como principio general por defecto, EXISTIRÁ una entrada por cada certificado X.509v3 (por ejemplo, para un servicio de certificación de tipo CA/QC) de los servicios de certificación de la lista de un CSP que figura en la Lista de Confianza (por ejemplo, una autoridad de certificación que expida (directamente) QC). En algunas circunstancias cuidadosamente estudiadas y en condiciones atentamente gestionadas y aprobadas, un organismo de supervisión/organismo de acreditación de un Estado miembro PODRÁ decidir utilizar el certificado X.509v3 de una CA raíz o CA de nivel superior (por ejemplo, una autoridad de certificación que no expida directamente QC a entidades finales, pero certifique una jerarquía de CA que descienda hasta las CA que expiden QC a entidades finales) como «Sdi» de una entrada única de la lista de servicios de un CSP de la lista. Los Estados miembros deberán estudiar y aprobar cuidadosamente las consecuencias (ventajas y desventajas) de utilizar este certificado X.509v3 de una CA raíz o CA de nivel superior como valor «Sdi» de entradas de servicios en la TL ([1]). Además, cuando se recurra a esta excepción autorizada al principio por defecto, los Estados miembros DEBERÁN aportar la documentación necesaria para facilitar la construcción y verificación de la trayectoria de certificación.

Nota: Los TSP tales como los respondedores OCSP y los expedidores CRL que forman parte de servicios de certificación de CSPQC y están sujetos al uso de pares de claves distintas para firmar, respectivamente, respuestas OCSP y CRL, PODRÁN figurar también en el presente modelo de TSL utilizando la siguiente combinación de URI:

— Valor «Service type identifier» (cláusula 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

combinado con el siguiente valor de la extensión additionalServiceInformation (cláusula 5.8.2) de «Service information extension» (cláusula 5.5.9):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Descripción: un proveedor de estado de certificación que opera un servidor OCSP como parte de un servicio de un CSP que expide certificados reconocidos.

— Valor «Service type identifier» (cláusula 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

combinado con el siguiente valor de la extensión additionalServiceInformation (cláusula 5.8.2) de «Service information extension» (cláusula 5.5.9):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Descripción: un proveedor de estado de certificación que opera una CRL como parte de un servicio de un CSP que expide certificados reconocidos.

— Valor «Service type identifier» (cláusula 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

([1]) Utilizar un certificado X.509v3 de CA raíz como valor «Sdi» para un servicio de la lista obligará al operador del régimen a considerar al conjunto de servicios de certificación que están bajo esa CA raíz como un todo con respecto al «estado de supervisión/acreditación». Por ejemplo, cualquier cambio de estado necesario para una única CA que esté bajo la jerarquía raíz de la lista obligará a recoger ese cambio de estado en toda la jerarquía.

▼C1

combinado con el siguiente valor de la extensión additionalServiceInformation (cláusula 5.8.2) de «Service information extension» (cláusula 5.5.9):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Descripción: una autoridad de certificación raíz a partir de la cual se puede establecer una trayectoria de certificación que descienda hasta una autoridad de certificación que expida certificados reconocidos.

— Valor «Service type identifier» (cláusula 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/TSA

combinado con el siguiente valor de la extensión additionalServiceInformation (cláusula 5.8.2) de «Service information extension» (cláusula 5.5.9):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Descripción: un servicio de estampación de fecha y hora dentro de un servicio de un proveedor de servicios de certificación que expide certificados reconocidos que expiden TST que pueden usarse en el proceso de verificación de firmas reconocidas para evaluar y extender la validez de la firma cuando se suprime el QC o expira.

Service name (cláusula 5.5.2)

Este campo es OBLIGATORIO y ESPECIFICARÁ el nombre con el cual el CSP identificado en «TSP name» (cláusula 5.4.1) presta el servicio identificado en «Service type identifier» (cláusula 5.5.1). CONSISTIRÁ en una secuencia de cadenas de caracteres multilingües (con el EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales).

Service digital identity (cláusula 5.5.3)

Este campo es OBLIGATORIO y ESPECIFICARÁ al menos una representación de un identificador digital único del servicio cuyo tipo se especifica en «Service type identifier» (cláusula 5.5.1) mediante el cual se pueda identificar sin ambigüedad el servicio.

En las presentes especificaciones, el identificador digital utilizado en este campo SERÁ el certificado X.509v3 pertinente que sea representación de la o las claves públicas que utiliza el CSP para prestar el servicio cuyo tipo especifica el «Service type identifier» (cláusula 5.5.1) (es decir, la clave usada por un CA raíz/QC, la clave usada para firmar certificados ([1]), o alternativamente para expedir sellos temporales, o firmar CRL, o firmar respuestas OCSP). Este certificado X.509v3 conexo SE UTILIZARÁ como identificador digital mínimo exigido (siendo la representación de la o las claves públicas que utiliza el CSP para prestar el servicio de la lista). PODRÁN utilizarse identificadores adicionales como se explica a continuación, pero todos DEBERÁN remitir a la misma identidad (es decir, el certificado X.509v3 conexo):

([1]) Puede tratarse del certificado de una CA que expide certificados de entidad final (por ejemplo, CA/PKC, CA/QC) o del certificado de una CA raíz de confianza desde la que puede encontrarse una trayectoria que descienda hasta los certificados reconocidos de entidad final. Dependiendo de si se puede o no utilizar esta información y la información que se encuentra en cada certificado de entidad final expedido bajo esta raíz de confianza para determinar sin ambigüedad las características apropiadas de cualquier certificado reconocido, podrá resultar necesario completar esta información («Service digital identity») con datos de «Service information extensions» (véase cláusula 5.5.9).

▼C1

a) la denominación distinguida (DN) del certificado que puede utilizarse para verificar las firmas electrónicas del servicio del CSP especificado en «Service type identifier» (cláusula 5.5.1);

b) el identificador de clave pública conexo (es decir, X.509v3 SubjectKeyIdentifier o valor SKI);

c) la clave pública conexa.

Como principio general por defecto, el identificador digital (es decir, el certificado X.509v3 conexo) NO ESTARÁ presente más de una vez en la Lista de Confianza, es decir, HABRÁ una entrada por cada certificado X.509v3 para un servicio de certificación de los servicios de certificación de la lista de un CSP que figura en la Lista de Confianza. A la inversa, un certificado X.509v3 SE UTILIZARÁ en una única entrada de servicio como valor «Sdi».

Nota (1): El único caso en que podrá no aplicarse el mencionado principio general por defecto es cuando se utilice un certificado X.509v3 único al expedir distintos tipos de tokens de servicios de confianza para los que se aplican regímenes de supervisión/acreditación diferentes, por ejemplo un CSP utiliza un certificado X.509v3 único por una parte cuando expide QC con arreglo a un sistema de supervisión adecuado y, por otra, cuando expide certificados no reconocidos con arreglo a un estado de supervisión/acreditación diferente. En este caso y ejemplo, se utilizarían dos entradas con valores «Sti» distintos (por ejemplo, respectivamente CA/QC y CA/PKC en el ejemplo dado) y con el mismo valor «Sdi» (el certificado X.509v3 conexo).

Las implementaciones son dependientes de ASN.1 o XML y SE AJUSTARÁN a las especificaciones ETSI TS 102 231 (para ASN.1 véase el anexo A de ETSI TS 102 231, y para XML véase el anexo B de ETSI TS 102 231).

Nota (2): Cuando sea necesario facilitar información adicional de «qualification» con respecto a la entrada del servicio identificado, el operador del régimen, si procede, CONSIDERARÁ la posibilidad de utilizar la extensión «additionalServiceInformation» (cláusula 5.8.2) del campo «Service information extension» (cláusula 5.5.9) a efectos de facilitar dicha información adicional. Además, el operador del régimen puede opcionalmente utilizar la 5.5.6 («Scheme service definition URI»).

Service current status (cláusula 5.5.4)

Este campo es OBLIGATORIO y ESPECIFICARÁ el identificador del estado del servicio a través de uno de los siguientes URI:

▼C2

— **Under Supervision** (Bajo supervisión) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— **Supervision of Service in Cessation** (Supervisión del servicio en proceso de suspensión) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— **Supervision Ceased** (Supervisión suspendida) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Supervision Revoked** (Supervisión suprimida) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

— **Accredited** (Acreditado) (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

— **Accreditation Ceased** (Acreditación suspendida) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **Accreditation Revoked** (Acreditación suprimida) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Estos estados SE INTERPRETARÁN, en el contexto de las presentes especificaciones de la Lista de Confianza, de la siguiente manera:

— ***Bajo supervisión:*** El servicio identificado en «Service digital identity» (cláusula 5.5.3) prestado por el proveedor de servicios de certificación (CSP) identificado en «TSP name» (cláusula 5.4.1) se encuentra actualmente bajo la supervisión, en cuanto al cumplimiento de lo dispuesto en la Directiva 1999/93/CE, del Estado miembro identificado en el «Scheme territory» (cláusula 5.3.10) en que está establecido el CSP.

▼M1

— ***Supervisión del servicio en proceso de suspensión:*** El servicio identificado en «Service digital identity» (cláusula 5.5.3) prestado por el CSP identificado en «TSP name» (cláusula 5.4.1) se encuentra actualmente en proceso de suspensión, pero sigue siendo supervisado hasta que se haya suspendido o suprimido la supervisión. En caso de que una persona jurídica distinta de la identificada en «TSP name» haya asumido la responsabilidad de garantizar este proceso de suspensión, SE FACILITARÁ la identificación de esta persona jurídica nueva o de reserva (CSP de reserva) en «Scheme service definition URI» (cláusula 5.5.6) y en la extensión «Taken over by» (cláusula L.3.2) de la entrada del servicio.

▼C1

— ***Supervisión suspendida:*** La validez de la evaluación de supervisión ha expirado sin que el servicio identificado en «Service digital identity» (cláusula 5.5.3) haya sido reevaluado. El servicio no se encuentra ya actualmente bajo supervisión a partir de la fecha del estado actual, pues se entiende que no está ya operativo.

— ***Supervisión suprimida:*** Aunque ha estado supervisado anteriormente, el servicio del CSP, y posiblemente el propio CSP, ha dejado de seguir cumpliendo lo dispuesto en la Directiva 1999/93/CE, según lo determinado por el Estado miembro identificado en el «Scheme territory» (cláusula 5.3.10) en el que está establecido el CSP. En consecuencia, se ha exigido al servicio que cese en sus actividades y debe considerarse suspendido por la razón mencionada.

Nota (1): El valor de estado «Supervisión suprimida» puede ser definitivo, incluso si el CSP abandona luego por completo su actividad; no es necesario migrar a los estados «Supervisión del servicio en proceso de suspensión» ni a «Supervisión suspendida» en este caso. En realidad, la única manera de alterar el estado «Supervisión suprimida» es pasar del no cumplimiento al cumplimiento de lo dispuesto en la Directiva 1999/93/CE con arreglo al sistema de supervisión apropiado vigente en el Estado miembro poseedor de la TL, y recuperar el estado «Bajo supervisión». Los estados «Supervisión del servicio en proceso de suspensión» y «Supervisión suspendida» solo se producen si un CSP extingue directamente sus servicios conexos bajo supervisión, no cuando se ha suprimido la supervisión.

— ***Acreditado:*** El organismo de acreditación ha efectuado una evaluación de acreditación en nombre del Estado miembro identificado en el «Scheme territory» (cláusula 5.3.10) y ha comprobado que el servicio identificado en «Service digital identity» (cláusula 5.5.3) prestado por el CSP ([1]) identificado en «TSP name» (cláusula 5.4.1) cumple lo dispuesto en la Directiva 1999/93/CE.

([1]) Nótese que este CSP acreditado puede estar establecido en un Estado miembro distinto del identificado en el «Scheme territory» de la implementación TSL de la TL o en un tercer país [véase el artículo 7, apartado 1, letra a), de la Directiva 1999/93/CE].

▼C1

Nota (2): Cuando se usa en el contexto de un CSP que expide QC que está establecido en el «Scheme territory» (cláusula 5.3.10), los estados «Acreditación suprimida» y «Acreditación suspendida» DEBERÁN considerarse «estados de tránsito» y NO DEBERÁN utilizarse como valor de «Service current status» pues, de utilizarse, DEBERÁN ir seguidos inmediatamente en la «Service approval history information» o en el «Service current status» por un estado «Bajo supervisión», seguido potencialmente de cualquier otro estado de supervisión definido anteriormente e ilustrado en la figura 1. Cuando se usa en el contexto de un CSP que no expide QC, cuando hay solo un régimen de «acreditación voluntaria» asociado, sin régimen de supervisión asociado, o en el contexto de un CSP que expide QC cuando el CSP no está establecido en el «Scheme territory» (cláusula 5.3.10) (por ejemplo, en un tercer país), PODRÁN utilizarse los estados de «Acreditación suprimida» y «Acreditación suspendida» como valor de «Service current status»:

— ***Acreditación suspendida:*** La validez de la evaluación de la acreditación ha expirado sin que el servicio identificado en «Service digital identity» (cláusula 5.5.3) haya sido reevaluado.

— ***Acreditación suprimida:*** Tras ser juzgado conforme con los criterios del régimen, el servicio identificado en «Service digital identity» (cláusula 5.5.3) prestado por el proveedor de servicios de certificación (CSP) identificado en «TSP name» (cláusula 5.4.1), y posiblemente el propio CSP, ha dejado de seguir cumpliendo lo dispuesto en la Directiva 1999/93/CE.

Nota (3): Deberán utilizarse exactamente los mismos valores de estado para los CSP que expiden QC y para los CSP que no expiden QC (por ejemplo, proveedores de servicios de estampación de fecha y hora que expiden TST, CSP que expiden certificados no reconocidos, etc.). Se utilizará el «Service Type identifier» (cláusula 5.5.1) para distinguir entre los sistemas de supervisión/acreditación aplicables.

Nota (4): PODRÁ facilitarse información adicional de «reconocimiento» relacionada con el estado definida a nivel de los sistemas nacionales de supervisión/-acreditación para los CSP que no expidan QC a nivel de servicio cuando proceda y resulte necesario (por ejemplo, para distinguir entre varios niveles de calidad/seguridad). Los operadores de regímenes UTILIZARÁN la extensión «additionalServiceInformation» (cláusula 5.8.2) del campo «Service information extension» (cláusula 5.5.9) a efectos de facilitar esta información adicional de «reconocimiento». Además, el operador del régimen puede usar la cláusula 5.5.6 («Scheme service definition URI»).

Current status starting date and time (cláusula 5.5.5)

Este campo es OBLIGATORIO y ESPECIFICARÁ la fecha y hora en la que se hizo efectivo el actual estado de aprobación (valor de fecha y hora según se define en ETSI TS 102 231 cláusula 5.1.4).

Scheme service definition URI (cláusula 5.5.6)

Este campo es OPCIONAL, y si está presente ESPECIFICARÁ el URI o los URI en que las partes usuarias pueden obtener la información específica del servicio facilitada por el operador del régimen en forma de secuencia de indicadores multilingües (con el EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales).

Si se utiliza, el URI o los URI referenciados DEBERÁN llevar a la información que describa el servicio según lo especificado por el régimen. En particular, esta información PODRÁ incluir, si procede:

a) un URI que indique la identidad del CSP de reserva en el caso de la supervisión de un servicio en proceso de suspensión en el que exista tal CSP de reserva (véase «Service current status» – cláusula 5.5.4);

▼C1

b) un URI que lleve a documentos que faciliten información adicional relacionada con el uso de algún reconocimiento específico definido a nivel nacional para un servicio supervisado/acreditado de suministro de tokens de servicio de confianza coherente con el uso del campo «Service information extension» (cláusula 5.5.9) con una extensión «additionalServiceInformation» como se define en la cláusula 5.8.2.

Service supply points (cláusula 5.5.7)

Este campo es OPCIONAL y, si está presente, ESPECIFICARÁ el URI o los URI en que las partes usuarias pueden acceder al servicio mediante una secuencia de cadenas de caracteres cuya sintaxis DEBERÁ ajustarse a RFC 3986.

TSP service definition URI (cláusula 5.5.8)

Este campo es OPCIONAL y, si está presente, ESPECIFICARÁ el URI o los URI en que las partes usuarias pueden obtener información específica del servicio facilitada por el TSP como secuencia de indicadores multilingües (con EN como lengua obligatoria y con, potencialmente, una o más lenguas nacionales). El URI o los URI referenciados DEBERÁN llevar a la información que describa el servicio según lo especificado por el TSP.

Service information extensions (cláusula 5.5.9)

En el contexto de las presentes especificaciones, este campo es OPCIONAL, pero ESTARÁ presente cuando la información facilitada en la «Service digital identity» (cláusula 5.5.3) no sea suficiente para identificar sin ambigüedad los certificados reconocidos expedidos por este servicio y/o la información presente en los certificados reconocidos conexos no permita la identificación procesable por máquina si el QC está o no respaldado por un SSCD ([1]).

En el contexto de las presentes especificaciones, cuando su uso sea OBLIGATORIO, por ejemplo, para servicios CA/QC, SE UTILIZARÁ un campo opcional de información «Service information extensions» («Sie»), estructurado, con arreglo a la extensión «Qualifications» definida en ETSI TS 102 231 anexo L.3.1, como secuencia de una o más tuplas, cada una de las cuales contendrá:

— información que se usará para precisar (filtros), dentro del servicio de certificación identificado en la «Sdi», el servicio concreto (es decir, conjunto de certificados reconocidos) para el que se exige/facilita información adicional con respecto a la presencia o ausencia de respaldo de SSCD (y/o expedición a personas jurídicas), y

— la información asociada («qualifiers») sobre si el conjunto de certificados reconocidos del servicio precisado está respaldado por un SSCD o no (cuando esta información es «QCSSCDStatusAsInCert», ello significa que esta información asociada forma parte del QC en una forma procesable por máquina y normalizada por el ETSI ([2])), o información sobre el hecho de que tales QC se expidan a personas jurídicas (por defecto deben considerarse expedidas solamente a personas físicas).

— QCWithSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): significa que está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o su organismo de acreditación) que cualquier QC expedido dentro del servicio (QCA) identificado en la «Service digital identity» (cláusula 5.5.3) y precisado por la información anterior (filtros) utilizada para precisar, dentro del servicio de certificación identificado en la «Sdi», el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la presencia o ausencia de respaldo de SSCD ESTÁ respaldado por un SSCD (es decir, que la clave privada asociada con la clave pública en el certificado se almacena en un dispositivo seguro de creación de firma conforme al anexo III de la Directiva 1999/93/CE);

([1]) Véase la sección 2.2 del presente documento.

([2]) Esto se refiere a una combinación adecuada de una declaración QcCompliance definida por el ETSI, declaraciones QcSSCD [ETSI TS 101 862] o una QCP/QCP + OID definida por el ETSI [ETSI TS 101 456].

▼C1

— QCNoSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): significa que está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o su organismo de acreditación) que cualquier QC expedido dentro del servicio (CA raíz/QC o CA/QC) identificado en la «Service digital identity» (cláusula 5.5.3) y precisado por la información anterior (filtros) utilizada para precisar, dentro del servicio de certificación identificado en la «Sdi», el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la presencia o ausencia de respaldo de SSCD NO ESTÁ respaldado por un SSCD (es decir, que la clave privada asociada con la clave pública en el certificado no se almacena en un dispositivo seguro de creación de firma conforme al anexo III de la Directiva 1999/93/CE);

— QCSSCDStatusAsInCert (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): significa que está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o su organismo de acreditación) que cualquier QC expedido dentro del servicio (CA/QC) identificado en la «Service digital identity» (cláusula 5.5.3) y precisado por la información anterior (filtros) utilizada para precisar, dentro del servicio de certificación identificado en la «Sdi», el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la presencia o ausencia de respaldo de SSCD CONTENDRÁ la información procesable por máquina que indique si el QC está o no respaldado por un SSCD;

— QCForLegalPerson (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): significa que está garantizado por el CSP y controlado (modelo de supervisión) o auditado (modelo de acreditación) por el Estado miembro (respectivamente su organismo de supervisión o su organismo de acreditación) que cualquier QC expedido dentro del servicio (QCA) identificado en la «Service digital identity» (cláusula 5.5.3) y precisado por la información anterior (filtros) utilizada para precisar, dentro del servicio de certificación identificado en la «Sdi», el conjunto concreto de certificados reconocidos para el que se exige esta información adicional con respecto a la expedición a una persona jurídica SE EXPIDE a personas jurídicas.

Estos «qualifiers» solo deben utilizarse como extensión, si el tipo de servicio es http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Este campo es específico de la implementación (ASN.1 o XML) y DEBERÁ cumplir las especificaciones contenidas en ETSI TS 102 231, anexo L.3.1.

▼M1

En el contexto de una implementación XML, el contenido específico de esta información adicional debe codificarse utilizando los archivos xsd que figuran en el anexo C de la ETSI TS 102 231.

▼C1

Service Approval History

Este campo es OPCIONAL, pero DEBERÁ estar presente si el «Historical information period» (cláusula 5.3.12) no es cero. Así pues, en el contexto de las presentes especificaciones, el régimen DEBERÁ conservar información histórica. En el caso de que deba conservarse dicha información, pero el servicio carezca de historia previa al estado actual (es decir, es el primer estado registrado o el operador del régimen no ha conservado información histórica) este campo ESTARÁ vacío. De no ser así, para cada modificación del estado actual del servicio del TSP sobrevenida dentro del período de información histórica según lo especificado en ETSI TS 102 231, cláusula 5.3.12, SE FACILITARÁ información sobre el estado de aprobación previo en orden descendente según la fecha y hora de modificación del estado (es decir, la fecha y la hora en que entró en vigor el estado de aprobación modificado).

▼C1

La secuencia de información histórica SE AJUSTARÁ a la definición siguiente.

TSP(1) Service(1) History(1)

Service type identifier (cláusula 5.6.1)

Este campo es OBLIGATORIO y ESPECIFICARÁ el identificador del tipo de servicio, con el formato y significado utilizado en «TSP Service Information – Service type identifier» (cláusula 5.5.1).

Service name (cláusula 5.6.2)

Este campo es OBLIGATORIO y ESPECIFICARÁ la denominación con la cual el CSP prestó el servicio identificado en «TSP Service Information – Service type identifier» (cláusula 5.5.1), con el formato y significado utilizados en «TSP Service Information – Service name» (cláusula 5.5.2). Esta cláusula no exige que la denominación sea la misma que la especificada en la cláusula 5.5.2. Un cambio de denominación PODRÁ ser una de las circunstancias que exijan un nuevo estado.

▼M1

Service digital identity (cláusula 5.6.3)

Este campo es OBLIGATORIO y ESPECIFICARÁ al menos una representación del identificador digital (por ejemplo, certificado X.509v3) utilizado en «TSP Service Information — Service digital identity» (cláusula 5.5.3) con el formato y el significado definidos en la ETSI TS 102 231, cláusula 5.5.3.

Nota: En relación con un determinado valor de certificado X.509v3 utilizado en la cláusula 5.5.3 «Service digital identity (Sdi)» de un servicio, debe haber en una lista de confianza una única entrada de servicio por valor «Sti:Sie/additionalServiceInformation». Los datos correspondientes a «Sdi» (cláusula 5.6.3) utilizados en la «service approval history information» asociada a una entrada de servicio y los datos «Sdi» (cláusula 5.5.3) utilizados en la presente entrada de servicio DEBERÁN estar relacionados con el mismo valor de certificado X.509v3. Cuando se esté modificando el «Sdi» de un servicio que figure en la lista (es decir, se proceda a la renovación o recodificación de un certificado X.509v3, por ejemplo un CA/PKC o CA/QC) o se esté creando un nuevo «Sdi» en relación con ese servicio, incluso con valores idénticos para los «Sti», «Sn», y [«Sie»] asociados, el operador del régimen DEBERÁ crear una entrada de servicio distinta de la anterior.

▼C1

Service previous status (cláusula 5.6.4)

Este campo es OBLIGATORIO y ESPECIFICARÁ el identificador del estado previo del servicio, con el formato y significado utilizado en «TSP Service Information – Service current status» (cláusula 5.5.4).

Previous status starting date and time (cláusula 5.6.5)

Este campo es OBLIGATORIO y ESPECIFICARÁ la fecha y hora en que entró en vigor el estado previo en cuestión, con el formato y significado utilizado en «TSP Service Information – Service current status starting date and time» (cláusula 5.5.5).

Service information extensions (cláusula 5.6.6)

Este campo es OPCIONAL y los operadores de regímenes PODRÁN utilizarlo para facilitar información relacionada con el servicio específico con el formato y significado utilizado en «TSP Service Information – Service information extensions» (cláusula 5.5.9).

▼C1

TSP(1) Service(1) History(2)

Idem para TSP(1) Service(1) History(2) (anterior a History 1)

…

TSP(1) Service(2)

Idem para TSP(1) Service 2 (si procede)

TSP(1)Service(2)History(1)

…

TSP(2) Information

Idem para TSP 2 (si procede)

Idem para TSP 2 Service 1

Idem para TSP 2 Service 1 History 1

…

▼M1

Signed TSL

La implementación TSL de la lista de confianza legible por personas establecida con arreglo a las presentes especificaciones, y, en particular, al capítulo IV, DEBERÍA ir firmada por el «Scheme operator name» (cláusula 5.3.4) a fin de garantizar su autenticidad e integridad ([1]). El formato de la firma DEBERÍA ser PAdES parte 3 (ETSI TS 102 778-3) ([2]), pero PODRÁ ser PAdES parte 2 (ETSI TS 102 778-2) ([3]) en el contexto del modelo de confianza específico establecido mediante la publicación de los certificados utilizados para firmar las listas de confianza.

La implementación TSL procesable por máquina de la lista de confianza establecida con arreglo a las presentes especificaciones ESTARÁ firmada por el «Scheme operator name» (cláusula 5.3.4) a fin de garantizar su autenticidad e integridad. El formato de la implementación TSL procesable por máquina de la lista de confianza, establecido con arreglo a las presentes especificaciones, SERÁ XML y SE ANTENDRÁ a las especificaciones establecidas en los anexos B y C de la ETSI TS 102 231.

El formato de la firma SERÁ XAdES BES o EPES tal como se definen en las especificaciones ETSI TS 101 903 para las implementaciones XML. Ese tipo de implementación de la firma electrónica CUMPLIRÁ los requisitos contemplados en el anexo B de la ETSI TS 102 231 ([4]). Los requisitos generales adicionales que deben reunirse en relación con la firma figuran en las secciones siguientes.

▼C1

Scheme identification (cláusula 5.7.2)

Este campo, que es OBLIGATORIO, ESPECIFICARÁ una referencia asignada por el operador del régimen que identifique de manera única el régimen descrito en las presentes especificaciones y la TSL establecida y DEBERÁ estar incluido en el cálculo de la firma. Se espera que se trate de una cadena de caracteres o de una cadena de bits.

([1]) En caso de que la implementación TSL legible por personas no vaya firmada, su autenticidad e integridad DEBERÁ garantizarse a través de un canal de comunicación apropiado dotado de un nivel de seguridad equivalente. A tal fin se recomienda la utilización de la TLS (IETF RFC 5246: «The Transport Layer Security (TLS) Protocol Version 1.2»), y el Estado miembro DEBERÁ poner a disposición de los usuarios de la TSL, fuera de banda, la huella del certificado del canal de la TSL.

([2]) ETSI TS 102 778-3 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced-PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic-Profile based on ISO 32000-1.

([4]) Es obligatorio proteger el certificado de firma del operador del régimen aplicando la firma de una de las formas que se especifican en ETSI TS 101 903 y el ds:keyInfo debe contener la cadena de certificado pertinente, en su caso.

▼M1

En el contexto de las presentes especificaciones, la referencia asignada INCLUIRÁ el «TSL type» (cláusula 5.3.3), el «Scheme name» (cláusula 5.3.6) y el valor de la extensión SubjectKeyIdentifier del certificado usado por el operador del régimen para firmar electrónicamente la TSL.

▼C1

Signature algorithm identifier (cláusula 5.7.3)

Este campo es OBLIGATORIO y ESPECIFICARÁ el algoritmo criptográfico que se ha utilizado para crear la firma. Dependiendo del algoritmo utilizado, este campo PODRÁ requerir parámetros adicionales. Este campo DEBERÁ estar incluido en el cálculo de la firma.

Signature value (cláusula 5.7.4)

Este campo es OBLIGATORIO y CONTENDRÁ el valor real de la firma digital. Todos los campos de la TSL (excepto el valor de la firma propiamente dicha) DEBERÁN estar incluidos en el cálculo de la firma.

TSL extensions (cláusula 5.8)

expiredCertsRevocationInfo (cláusula 5.8.1)

Esta extensión es OPCIONAL. Si se utiliza, DEBERÁ ajustarse a las especificaciones de ETSI TS 102 231, cláusula 5.8.1.

additionalServiceInformation (cláusula 5.8.2)

Esta extensión OPCIONAL. Cuando se utilice, DEBERÁ usarse solamente a nivel de servicio y solamente en el campo definido en la cláusula 5.5.9 («Service information extension»). Se utiliza para facilitar información adicional sobre un servicio. SERÁ una secuencia de una o más tuplas, cada una de las cuales contendrá:

a) un URI que identifique la información adicional, por ejemplo:

   — un URI que indique algún reconocimiento específico definido a nivel nacional para un servicio supervisado/acreditado de suministro de tokens de servicio de confianza, por ejemplo,

      — un nivel de granularidad de la calidad/seguridad específico con respecto al régimen de supervisión/acreditación nacional para los CSP que no expidan QC (por ejemplo, RGS */**/*** en FR, un estado de «supervisión» específico fijado por la legislación nacional para CSP específicos que expiden QC en DE), véase la nota (4) de «Service current status» – cláusula 5.5.4,

      — o un estado legal específico para el suministro de tokens de servicio de confianza supervisado/acreditado (por ejemplo, «TST reconocido» definido a nivel nacional, como en DE o HU),

      — o un identificador de política específica presente en un certificado X.509v3 facilitado en el campo «Sdi».

   — o un URI registrado según se especifica en el «Service type identifier», cláusula 5.5.1, a fin de precisar la participación del servicio identificado en «Sti» en tanto que servicio componente de un proveedor de servicios de certificación que expide QC (por ejemplo, OCSP-QC, CRL-QC, y CA raíz-QC);

b) una cadena opcional que contenga el valor serviceInformation, según lo especificado en el régimen (por ejemplo, *, ** o ***);

c) cualquier información adicional opcional facilitada en un formato específico del régimen.

▼M1

La desreferenciación del URI DEBERÍA permitir disponer de información legible por personas (como mínimo en inglés y, potencialmente en uno o varios idiomas nacionales) que se considere suficiente y apropiada para que una determinada parte usuaria comprenda la extensión, y, en particular, que explique el significado de los URI dados, especificando los posibles valores de serviceInformation y el significado de cada uno de ellos.

Qualifications Extension (cláusula L.3.1)

Descripción: Este campo es OPCIONAL, pero ESTARÁ presente cuando su uso sea OBLIGATORIO, por ejemplo, para servicios CA raíz/QC o CA/QC, y cuando

— la información facilitada en la «Service digital identity» no sea suficiente para identificar sin ambigüedad los certificados reconocidos expedidos por este servicio,

— la información presente en los certificados reconocidos conexos no permita la identificación procesable por máquina de los hechos que determinan si el QC está o no respaldado por un SSCD.

Cuando se utilice, esta extensión del nivel de servicio solo DEBERÁ aplicarse en el ámbito definido en «Service information extension» (cláusula 5.5.9) y CUMPLIRÁ las especificaciones establecidas en el anexo L.3.1 de ETSI TS 102 231.

Extensión TakenOverBy (cláusula L.3.2)

Descripción: Esta extensión es OPCIONAL, pero ESTARÁ presente cuando un servicio que se encuentre previamente bajo la responsabilidad de un CSP sea asumido por otro TSP, y su finalidad es mostrar en quién recae la responsabilidad jurídica de un determinado servicio y permitir que el software de comprobación revele al usuario cierta información de tipo jurídico. La información facilitada en esta extensión DEBERÁ guardar coherencia con la utilización de la cláusula 5.5.6 y DEBERÁ cumplir las especificaciones previstas en el anexo L.3.2 de ETSI TS 102 231.

▼**M1**

CAPÍTULO II

En la elaboración de sus listas de confianza, los Estados miembros utilizarán:

códigos de lengua en minúsculas y códigos de país en mayúsculas;

códigos de lengua y códigos de país de conformidad con el cuadro que figura a continuación.

En los casos en que figure un alfabeto latino (con su código de lengua pertinente) se incluirá una transliteración al alfabeto latino con los códigos de lengua correspondientes, especificados en el cuadro que aparece a continuación.

Denominación usual (en lengua original)	Denom. Usual (en inglés)	Código de país	Código de lengua	Notas	Transliteración al alfabeto latino
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Código de país recomendado por la UE	el-Latn
España	Spain	ES	es	También catalán (ca), Vasco (eu) y gallego (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼**M1**

Denominación usual (en lengua original)	Denom. Usual (en inglés)	Código de país	Código de lengua	Notas	Transliteración al alfabeto latino
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Código de país recomendado por la UE	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Transliteración en caracteres latinos: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

CAPÍTULO IV

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

DEBERÁ existir una forma legible por personas (*Human Readable* o HR) de la implementación TSL de la lista de confianza disponible para el público y accesible por medios electrónicos. DEBERÍA facilitarse en forma de documento PDF con arreglo a ISO 32000 que DEBERÁ estar formateado de acuerdo con el perfil PDF/A (ISO 19005).

El contenido de la forma HR basada en PDF/A de la implementación TSL de la Lista de Confianza DEBERÍA cumplir los siguientes requisitos:

▼M1

— el título de la versión de las listas de confianza legible por personas deberá configurarse como una concatenación de los siguientes elementos:

  — con carácter facultativo, una imagen de la bandera nacional del Estado miembro,

  — un espacio en blanco,

  — la denominación usual del país en la lengua o lenguas de origen (tal como figura en la primera columna del cuadro del capítulo II),

  — un espacio en blanco,

  — «(»,

  — la denominación usual del país en inglés (tal como figura en la segunda columna del cuadro del capítulo II) dentro del paréntesis,

  — «):» como cierre del paréntesis y separación,

  — un espacio en blanco,

  — «Lista de confianza»,

  — con carácter facultativo, el logotipo del operador del régimen del Estado miembro.

▼C1

— La estructura de la forma HR DEBERÍA reflejar el modelo lógico descrito en la sección 5.1.2 de ETSI TS 102 231.

— DEBERÍAN presentarse todos los campos presentes, que facilitarían:

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

  — el valor del campo (por ejemplo, «CA/QC»);

  — el significado (descripción) del valor del campo, si procede y en particular según lo previsto en el anexo D de ETSI TS 102 231 o en las presentes especificaciones para los URI registrados (por ejemplo, «una autoridad de certificación que expide certificados de clave pública»);

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

— DEBERÍAN presentarse como mínimo en la forma HR los siguientes campos y valores correspondientes de los certificados digitales presentes en el campo «Service digital identity»:

  — versión

  — número de serie

  — algoritmo de firma

  — expedidor

  — válido a partir del

  — válido hasta el

  — sujeto

▼C1

— clave pública

— políticas de certificados

— identificador de clave de sujeto

— puntos de distribución CRL

— identificador de clave de autoridad

— uso de claves

— restricciones básicas

— algoritmo de huella digital

— huella digital.

— La forma HR DEBERÍA ser fácilmente imprimible.

— La forma HR PODRÁ estar firmada electrónicamente. En tal caso, DEBERÁ estarlo por el operador del régimen con arreglo a las mismas especificaciones en cuanto a la firma que la implementación TSL de la lista de confianza.