DECISIÓN DE EJECUCIÓN DE LA COMISIÓN

de 14 de octubre de 2013

por la que se modifica la Decisión 2009/767/CE en lo relativo al establecimiento, el mantenimiento y la publicación de listas de confianza de proveedores de servicios de certificación supervisados o acreditados por los Estados miembros

[notificada con el número C(2013) 6543]

(Texto pertinente a efectos del EEE)

(2013/662/UE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión 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) La Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las «ventanillas únicas» con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y el Consejo relativa a los servicios en el mercado interior [2], exige a los Estados miembros que difundan la información necesaria para la validación de firmas electrónicas avanzadas respaldadas por un certificado reconocido. Esta información debe presentarse de manera uniforme utilizando las denominadas «listas de confianza», que contienen información sobre los proveedores de servicios de certificación que expiden al público certificados reconocidos de conformidad con la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica [3], y son supervisados y acreditados por los Estados miembros.

(2) La experiencia práctica respecto a la ejecución de la Decisión 2009/767/CE por los Estados miembros ha puesto de relieve que se requieren ciertas mejoras para aprovechar al máximo las ventajas de las listas de confianza. Además, el Instituto Europeo de Normas de Telecomunicación (ETSI) ha publicado nuevas especificaciones técnicas relativas a las listas de confianza (TS 119 612), basadas en las especificaciones incluidas actualmente en el anexo a la Decisión, pero que, al mismo tiempo, incorporan diversas mejoras respecto a las especificaciones existentes.

(3) Por tanto, la Decisión 2009/767/CE debe modificarse para hacer referencia a las especificaciones técnicas 119 612 del ETSI e incorporar los cambios considerados necesarios para mejorar y facilitar el establecimiento y la utilización de las listas de confianza.

(4) A fin de que los Estados miembros puedan introducir en sus listas de confianza los cambios técnicos oportunos, resulta adecuado que la presente Decisión se aplique a partir del 1 de febrero de 2014.

(5) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité de la Directiva de Servicios.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Modificaciones de la Decisión 2009/767/CE

La Decisión 2009/767/CE se modifica como sigue:

1) El artículo 2 queda modificado como sigue:

a) los apartados 1, 2 y 2 *bis* se sustituyen por el texto siguiente:

«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, al menos, la información referente a los proveedores de servicios de certificación que expiden certificados reconocidos al público por él supervisados/acreditados.

2. Los Estados miembros elaborarán y publicarán una versión de la lista de confianza procesable por máquina, de conformidad con las especificaciones que figuran en el anexo. Si un Estado miembro opta por publicar una versión legible por las personas de su lista de confianza, dicha versión se atendrá a 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 a fin de garantizar su autenticidad e integridad. Si un Estado miembro publica una versión legible por las personas de la lista de confianza, se asegurará de que dicha versión contenga los mismos datos que la versión procesable por máquina, y la firmará electrónicamente con el mismo certificado utilizado para esta última.»;

[1] DO L 376 de 27.12.2006, p. 36.
[2] DO L 274 de 20.10.2009, p. 36.
[3] DO L 13 de 19.1.2000, p. 12.

b) se inserta el apartado 2 *ter* siguiente:

«*2 ter*. Los Estados miembros se asegurarán de que la versión procesable por máquina de sus respectivas listas de confianza sea accesible en su lugar de publicación en todo momento, sin interrupción, excepto con fines de mantenimiento.»;

c) el apartado 3 se sustituye por el texto siguiente:

«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 la versión de su lista de confianza procesable por máquina;

b) el lugar en el que figura publicada la versión procesable por máquina de la lista de confianza;

c) dos o más certificados de clave pública de operadores de regímenes, con un desfase mínimo de tres meses entre sus períodos de vigencia, que correspondan a las claves privadas que pueden utilizarse para firmar electrónicamente la versión procesable por máquina de la lista de confianza;

d) cualquier cambio introducido en la información indicada en las letras a), b) y c).»;

d) se inserta el apartado 3 *bis* siguiente:

«3 *bis*. Si un Estado miembro publica una versión legible por personas de la lista de confianza, la información a la que se refiere el apartado 3 se notificará asimismo respecto a esta versión.»

2) El anexo se sustituye por el anexo de la presente Decisión.

Artículo 2

Aplicación

La presente Decisión será aplicable a partir del 1 de febrero de 2014.

Artículo 3

Destinatarios

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 14 de octubre de 2013.

Por la Comisión

Michel BARNIER

Miembro de la Comisión

ANEXO

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

REQUISITOS GENERALES

1. **Introducción**

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 [*certification services providers* ([1]) o CSP] que supervisa/acredita en cuanto al cumplimiento de las disposiciones pertinentes de la Directiva 1999/93/CE. Ello incluye la presentación de información histórica sobre el estado de supervisión/acreditación de los servicios de certificación supervisados/acreditados.

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) ([2]) respaldadas por un certificado reconocido ([3]) ([4]).

La información obligatoria de la lista de confianza (*Trusted List* o TL) deberá incluir. como mínimo, información sobre los CSP supervisados/acreditados que expiden certificados reconocidos (*Qualified Certificates* o QC) ([5]) 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, cuando no forma parte de los QC, 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) ([6]).

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.), siempre que se acrediten o supervisen de un modo similar al de los CSP que expiden QC, o hayan sido autorizados con arreglo a un régimen de aprobación nacional diferente. Es posible que los regímenes de aprobación nacionales en algunos Estados miembros difieran de los regímenes de supervisión o de acreditación voluntaria aplicables a los CSP que expiden QC en lo que atañe a los requisitos exigibles y/o la organización competente. Los términos «acreditado» y/o «supervisado» en las presentes especificaciones también atañen a los regímenes de aprobación nacionales, pero los Estados miembros deberán facilitar información adicional sobre la naturaleza de sus regímenes nacionales en sus respectivas listas de confianza, incluida una aclaración sobre las posibles diferencias con los regímenes de acreditación/supervisión aplicados a los CSP que expiden QC.

El modelo común se basa en la norma ETSI TS 119 612 v1.1.1 ([7]) (a la que se aludirá en lo sucesivo como ETSI TS 119 612), que se refiere al establecimiento, la publicación, la localización, el acceso, la autenticación y la integridad de tales listas.

2. **Estructura del modelo común de la lista de confianza**

El modelo común de la lista de confianza de un Estado miembro se estructura con arreglo a la ETSI TS 119 612, en las siguientes categorías de información:

1. una etiqueta de lista de confianza que facilite la identificación de la esta lista en las búsquedas electrónicas;

2. información sobre la lista de confianza y su régimen de expedición;

3. una secuencia de campos que contenga información de identificación inequívoca sobre cada uno de los CSP supervisados/acreditados en virtud del régimen (esta secuencia es opcional, es decir, si no se usa, se considerará que la lista carece de contenido, lo que significará que no hay ningún CSP supervisado o acreditado en el Estado miembro correspondiente por lo que se refiere a la lista de confianza);

4. respecto a cada CSP incluido en la Lista, los datos pormenorizados de sus servicios de confianza específicos, cuya estado actual se registra en la lista de confianza, se facilitan mediante una secuencia de campos que identifican de manera inequívoca los servicios de certificación supervisados/acreditados que presta el CSP y su estado actual (esta secuencia debe contener, al menos, una entrada);

([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 2, de la Directiva 1999/93/CE.
([3]) Para referirse a una AdES respaldada por un QC se utiliza en el presente documento el acrónimo «$AdES_{QC}$».
([4]) 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.
([5]) Según se define en el artículo 2, punto 10, de la Directiva 1999/93/CE.
([6]) Según se define en el artículo 2, punto 6, de la Directiva 1999/93/CE.
([7]) ETSI TS 119 612 v1.1.1 (2013-06) — *Electronic Signatures and Infrastructures (ESI); Trusted Lists*.

5. respecto a cada servicio de certificación supervisado/acreditado incluido en la lista, la información sobre el historial de tal estado, en su caso;

6. la firma aplicada en la lista de confianza.

En el caso de un CSP que expide QC, la estructura de la lista de confianza y, en particular, el componente relativo a la información de los servicios (con arreglo al punto 4 anterior) permite que la información complementaria en las extensiones de información de servicio compense aquellas situaciones en las que se dispone de una información (procesable por máquina) insuficiente en el certificado reconocido respecto a su estado «reconocido», o su posible respaldo por un SSCD y, en especial, con el fin de atender al hecho adicional de que la mayoría de los CSP (comerciales) utilizan una única autoridad de certificación (*Certification Authority*, CA) para expedir diversos tipos de certificados de entidad final, tanto reconocidos, como no reconocidos.

En el contexto de los servicios de generación de certificados (CA), el número de entradas de servicios en la lista correspondiente a un CSP puede reducirse en el caso de que existan uno o varios servicios CA de nivel superior en la PKI del CSP (por ejemplo, en el contexto de una jerarquía de CA que descienda desde una CA raíz, a varias CA expedidoras), mediante la inclusión en la lista pertinente de los servicios CA superiores, y no de los servicios CA que expiden certificados de entidad final (por ejemplo, consignando en la lista únicamente la CA raíz del CSP). No obstante, en tales casos, la información del estado se aplica al conjunto de la jerarquía de servicios CA por debajo del servicio de la lista, y ha de mantenerse y asegurarse el principio de garantizar el vínculo inequívoco entre un servicio de certificación CSP_{QC} y el conjunto de certificados que se desea se identifiquen como QC.

2.1. *Descripción de la información en cada categoría*

1. Etiqueta de lista de confianza

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

Forma parte de esta categoría la información siguiente:

— un **identificador de versión del formato** de la lista de confianza,

— un **número de secuencia (o de versión)** de la lista de confianza,

— **información sobre el tipo** de lista de confianza (por ejemplo, para indicar que esta lista 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),

— **información sobre el operador del régimen (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 y/o aviso legal y responsabilidades** de la lista de confianza,

— **fecha y lugar de expedición** de la lista de confianza,

— **próxima actualización prevista** de la lista de confianza.

3. Información de identificación inequívoca sobre cada CSP supervisado/acreditado 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 (incluido 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 adicional.

4. Para cada CSP de la lista, una secuencia de campos que contengan una identificación inequívoca 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:

— identificador del tipo de servicio: 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) del servicio: nombre (comercial) de este servicio de certificación,

— identidad digital del servicio: un identificador único e inequívoco del servicio de certificación,

— estado actual del servicio: un identificador del estado actual del servicio,

— fecha y hora de inicio del estado actual,

— extensión de información del servicio, en su caso: información adicional sobre el servicio (por ejemplo, incluida directamente o indicando algún lugar del que pueda descargarse tal información); información de definición del servicio facilitada por el operador del régimen, información de acceso relativa al servicio, información de definición del servicio facilitada por el CSP y extensiones de información del servicio; por ejemplo, para los servicios CA/QC, una secuencia opcional de tuplas de información, en la que cada tupla contiene:

  — los criterios que deben utilizarse para precisar (filtrar) dentro del servicio de confianza identificado, el conjunto concreto de resultados del servicio [es decir, el conjunto de certificados (reconocidos)] para el que se exige/facilita información adicional con respecto a la indicación del respaldo por SSCD y/o expedición a una persona jurídica, y

  — los «qualifiers» asociados que faciliten información sobre si el conjunto de resultados del servicio identifica certificados que deban considerarse como reconocidos, y/o si los certificados reconocidos identificados de este servicio están respaldados por un SSCD o no, y/o información sobre si tales QC se expiden a una persona jurídica (por defecto deben considerarse expedidos a personas físicas).

5. Para cada servicio de certificación de la Lista, la información histórica sobre su estado

6. Una firma computada a efectos de autenticación respecto a todos los campos de la TL, excepto el valor de la firma en sí

3. **Directrices para la edición de las entradas de la lista de confianza**

3.1. *Información sobre el estado de supervisión/acreditación de los servicios de certificación y sus proveedores en una única lista*

La lista de confianza de un Estado miembro equivale a 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».

Esa lista de confianza es el único instrumento que debe utilizar cada Estado miembro para facilitar información sobre el estado de supervisión/acreditación de los servicios de certificación y sus proveedores:

— **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, 11, 12 y 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) y/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 1993/93/CE).

— Algunos de los objetos físicos o binarios (lógicos) generados o expedidos como resultado 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.

Deberá establecerse y mantenerse una única lista de confianza por Estado miembro para indicar el estado de supervisión y/o acreditación de los servicios de certificación de los CSP que están supervisados/acreditados por el Estado miembro. La lista de confianza incluirá al menos aquellos CSP que expiden QC. Podrá indicar asimismo el estado de otros servicios de certificación supervisados o acreditados en el marco de un régimen de aprobación definido a escala nacional.

3.2. *Un conjunto único de valores sobre el estado de supervisión/acreditación*

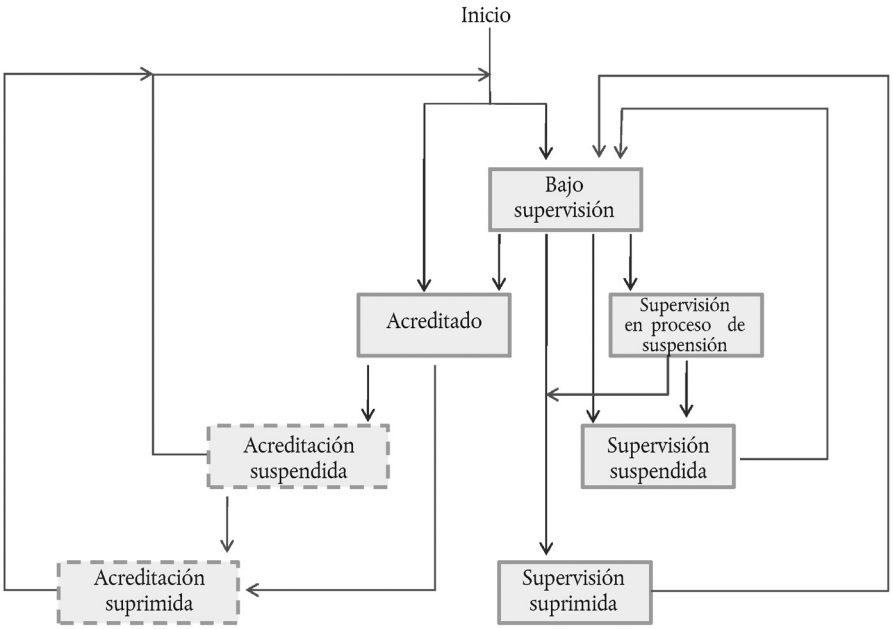
En la lista de confianza, el hecho de que un servicio se encuentre en cada momento «supervisado» o «acreditado» viene dado por el valor de su estado actual. Además, un estado de supervisión o acreditación puede ser positivo («bajo supervisión», «acreditado», «supervisión en proceso de suspensión») o estar suspendido («supervisión suspendida», «acreditación suspendida»), o incluso suprimido («supervisión suprimida», «acreditación suprimida»), y establecerse en el valor correspondiente. 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 y/o económicas.

Figura 1

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



Leyenda:

Estado de tránsito cuando hay un modelo de superv isión asociado (p. ej., para un CSP que expide QC y está acreditado y superv isado en el Estado miembro en el que se encuentra establecido).
Posible estado actual cuando no hay un modelo de superv isión asociado (p. ej., para un CSP acreditado en un Estado miembro en el que no está establecido).

Posible estado actual.

Si se encuentra establecido en un Estado miembro, un servicio de certificación que expida QC deberá ser supervisado (por el Estado miembro en el que esté establecido), y podrá ser acreditado voluntariamente. El valor del estado de tal servicio cuando conste en una lista de confianza debe ser uno de los valores antes indicados como «valor actual del estado», con arreglo a su estado efectivo, y deberá modificarse, en su caso, con arreglo al flujo de estado descrito en la figura anterior. Sin embargo, «acreditación suspendida» y «acreditación suprimida» deberán ser valores de «estado de tránsito» cuando el servicio CSP_{QC} conste en la lista de confianza del Estado miembro en el que se encuentra establecido, ya que tal servicio deberá estar supervisado por defecto (incluso si no está acreditado, o ha dejado de estarlo); cuando el servicio correspondiente figure en la lista (acreditado) en otro Estado miembro distinto de aquel en el que se encuentre establecido, tales valores podrán ser definitivos.

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.

Por consiguiente, un servicio de certificación que no expida QC podrá ser supervisado o acreditado voluntariamente. El valor del estado de tal servicio cuando conste en una lista de confianza debe ser uno de los valores antes indicados como su «valor de estado actual» (véase la figura 1), con arreglo a su estado efectivo, y deberá modificarse, en su caso, con arreglo al flujo de estado descrito en la figura anterior.

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 lista de confianza 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 lista de confianza 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 5.5.9.4) dentro de la «Service information extensions» (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 y que su estado de supervisión/acreditación se actualice en consecuencia.

3.3. *Entradas de la lista de confianza cuyo objetivo es facilitar la validación de QES y $AdES_{QC}$*

La parte más crítica de la creación de la lista de confianza 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 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).

La información exigida podría incluir información distinta de la «Service digital identity» de una única CA (raíz), en particular información que identifique el estado de QC de los certificados expedidos por tal servicio CA, 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 lista de confianza deberá tener en cuenta, por tanto, el perfil actual y el contenido del certificado en cada QC expedido, por cada servicio CSP_{QC} incluido en la lista de confianza.

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, y/o que cada QC expedido incluye uno de los identificadores de objeto (*Object Identifier* u OID) de política de certificados QCP/QCP + definido en ETSI EN 319.411-2 ([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.

([1]) Para una definición de tal declaración, véase ETSI EN 319 412-5 (*Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile*).

([2]) ETSI EN 319.411-2-*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.*

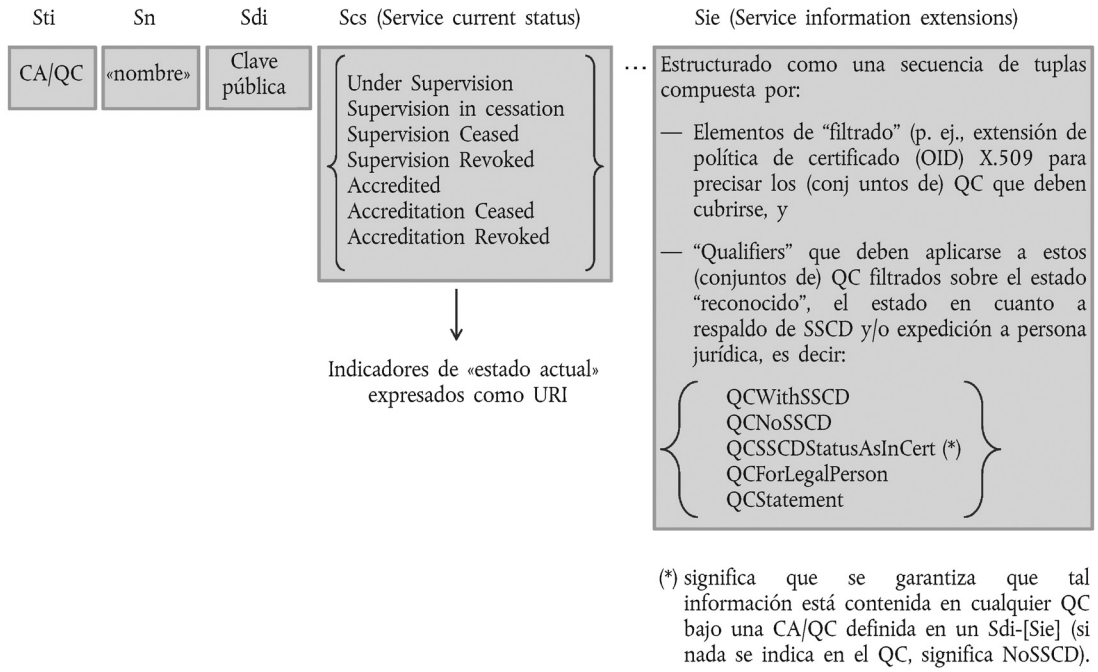
Rellenar los campos «Service type identifier» («Sti»), «Service name» («Sn») y «Service digital identity» («Sdi») de la entrada de servicio en la lista de confianza con la información facilitada en el campo «Service information extensions» («Sie») permite la determinación íntegra de un tipo específico de certificado reconocido expedido por un servicio de certificación de un CSP que expide QC que figura en la lista, y facilita información sobre si está respaldado o no por un SSCD (cuando tal información está ausente del QC expedido). 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 respaldado por un SSCD), la inclusión en la lista solo del «Sdi» de esa CA (raíz) permite únicamente asumir que un QC expedido bajo esta (jerarquía de) CA (raíz) no está respaldado por ningún SSCD. Para indicar que tales QC deben considerarse respaldados por un SSCD, debería utilizarse el campo «Sie» (lo que indica también que esa información está garantizada por el CSP que expide los QC y está supervisada/acreditada por el organismo de supervisión o acreditación respectivamente).

Figura 2

Entrada de un servicio de un CSP que expide QC y figura en la lista de confianza

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



Las presentes especificaciones técnicas del modelo común de la lista de confianza 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, la clave pública (como mínimo) de una CA que expide QC,

— para los servicios CA/QC, información opcional «Service information extension» («Sie») que permitirá la inclusión de varios datos específicos relacionados con el servicio y relativos al estado de supresión de certificados expirados, características adicionales de QC, la absorción de un CSP por otro CSP, y otros datos adicionales sobre los servicios. Por ejemplo, las características adicionales de los QC se representan mediante una secuencia de una o varias tuplas, cada una de las cuales contendrá:

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

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

— 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.

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

Las **directrices generales de edición** son las siguientes:

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 y/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 y/o el OID QCP, y no contiene 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 un certificado respaldado por un SSCD 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 y/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 reconocimiento. Es probable que ello exija la inclusión de «SSCD support information values» diferentes para la misma «Sdi» cuando se haga uso del campo «Sie».

Como principio general por defecto, para un CSP que figure en la lista de confianza deberá haber una entrada de servicio por cada clave pública única para un servicio de certificación de tipo CA/QC, es decir, una autoridad de certificación que expida (directamente) QC. En ciertas circunstancias excepcionales y en condiciones cuidadosamente gestionadas, el

organismo de supervisión o acreditación del Estado miembro podrá optar por utilizar, como el «Sdi» de una entrada única en la lista de servicios del CSP de la lista, la clave pública de un CA raíz o de nivel superior en la PKI del CSP (por ejemplo, en el contexto de la jerarquía del CSP de CA que descienda desde una CA raíz, a varias CA expedidoras), en lugar de incluir en la lista todos los servicios CA expedidores subordinados (es decir, incluir en la lista 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). Las consecuencias (ventajas y desventajas) de utilizar esta clave pública de una CA raíz o CA de nivel superior como valor «Sdi» en una entrada de servicio en la lista de confianza deberán ser consideradas con detenimiento cuando los Estados miembros procedan a su aplicación. 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. Como ejemplo, 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 este CA raíz está respaldado por un SSCD. Si estos QC están realmente respaldados por un SSCD, pero sin ninguna declaración procesable por máquina que indique que tal respaldo se incluye en los certificados, se recomendaría encarecidamente hacer uso de la declaración QcSSCD en los QC que se expidan en el futuro. Mientras tanto (hasta que haya expirado el último QC que no contenga esta información), la lista de confianza debería hacer uso del campo «Sie» y la extensión «Qualifications» asociada, por ejemplo, facilitando información de filtrado para identificar los conjuntos de certificados mediante el uso de OID específicos definidos por el CSP_{QC} y utilizados potencialmente por el CSP_{QC} para distinguir entre distintos tipos de QC (unos respaldados por un SSCD y otros no), asociando una «SSCD support information» explícita con estos conjuntos de certificados (filtrados) identificados mediante el uso de «Qualifiers».

Las **directrices generales de uso** para las aplicaciones, servicios o productos de firma electrónica que se basan en una lista de confianza conforme 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 procesables por máquina (es decir, QcCompliance), y/u 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 de la extensión «Qualification» de «Sie» o si un certificado de entidad final del que se afirma es un QC no se precisa mediante una extensión «Qualification» de «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, QcCompliance, QcSSCD) y/u OID QCP(+) definidos por el ETSI es conforme a lo que afirma el CSP_{QC},

— **y SI** hay presente información de la extensión «Qualification» de «Sie», entonces además de la regla de interpretación de uso por defecto precedente, los certificados que se identifican mediante el uso de tal información, que se construye con arreglo al principio de una secuencia de filtros que precisa un conjunto de certificados, deben considerarse con arreglo al conjunto de «qualifiers» asociados, facilitando alguna información adicional sobre el «respaldo por SSCD» y/o «persona jurídica como sujeto» (por ejemplo, los certificados que contienen un OID específico en la extensión de política de certificado, y/o tienen un patrón específico de «Key usage», y/o filtrados mediante el uso de un valor específico que aparece en un campo concreto o extensión del certificado, etc.). Tales «qualifiers» forman parte del siguiente conjunto de «qualifiers» utilizados para compensar la ausencia de información en el contenido del QC correspondiente, y que se utilizan respectivamente:

  — para indicar el estado de reconocido: «QCStatement», lo que significa que los certificados identificados están reconocidos,

    Y/O

  — para indicar la naturaleza del respaldo de 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,

    Y/O

— para indicar expedición a persona jurídica:

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

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

Los servicios de estado de validez de certificados relacionados con los QC, y con respecto a los cuales la información sobre el estado de validez de un certificado (por ejemplo, CRL y respuestas OCSP) sea firmada por una entidad cuya clave privada no está certificada con arreglo a una trayectoria de certificación que conduzca a una CA que expida QC y se incluya en la lista («CA/QC»), se incluirán en la lista de confianza mediante su consignación como tales en dicha lista (es decir, con un tipo de servicio «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 al 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»).

La lista de confianza incluirá servicios de estado de validez de certificados cuando la información de localización relacionada de tales servicios no figure en los certificados de entidad final a los que se apliquen dichos servicios.

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	1) un proveedor de servicios de certificación que crea y asigna certificados de clave pública, o 2) un servicio técnico de generación de certificados utilizado por un proveedor de servicios de certificación que crea y asigna certificados de clave pública. *Nota:* Véase la cláusula 4 de EN 319 411-2 [1] para una explicación más amplia del concepto de autoridad de certificación.
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	Alude a la supervisión prevista en el artículo 3, apartado 3, de la Directiva 1999/93/CE. 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.

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 119.612.
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 119 612). *Nota:* este término se utiliza en un sentido más amplio que el de servicio de certificación que expide certificados o presta otros servicios relacionados con las firmas electrónicas.
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 como resultado del uso de un servicio de confianza. Ejemplos de TrST binarios son los certificados, las listas de supresión de certificados (CRL), los tokens de sello temporal (TST) y las respuestas OCSP (*Online Certificate Status Protocol*).
Firma electrónica reconocida	QES	Una AdES respaldada por un QC y que se crea mediante un dispositivo seguro de creación de firma, 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 una 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.

([1]) EN 319 411-2: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.*

En los capítulos siguientes, 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]).

CAPÍTULO I

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

Las presentes especificaciones se basan en las especificaciones y requisitos contenidos en la norma ETSI TS 119 612 v1.1.1 (a la que se alude en lo sucesivo como ETSI TS 119 612).

Cuando en las presentes especificaciones no figure ningún requisito específico, se APLICARÁN íntegramente los requisitos de las cláusulas 5 y 6 de la ETSI TS 119 612. Cuando figuren requisitos específicos, estos PREVALECERÁN sobre los requisitos correspondientes de ETSI TS 119 612. En caso de discrepancia entre las presentes especificaciones y las especificaciones de ETSI TS 119 612, las primeras SERÁN las normativas.

Scheme operator name (cláusula 5.3.4)

Este campo DEBERÁ estar presente y cumplir las especificaciones previstas en la cláusula 5.3.4 de TS 119 612.

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

Un país PODRÁ tener organismos de supervisión y acreditación distintos e incluso organismos adicionales para las eventuales actividades operativas conexas. Compete a cada Estado miembro designar al operador del régimen de su lista de confianza. 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 lista de confianza, incluida la información específica del régimen indicada por el «Scheme information URI» (cláusula 5.3.7).

Scheme name (cláusula 5.3.6)

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

«EN_name_value» = «Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator's Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.»

Scheme information URI (cláusula 5.3.7)

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

— información introductoria 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 debe utilizarse es el que figura a continuación, en el que la cadena de caracteres «[*name of the relevant Member State*]» SERÁ sustituida por el nombre del Estado miembro pertinente:

«The present list is the "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;

— allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including, when this is not part of the QCs, 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 compliance 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 Article 3(3), Article 8.(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 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},

  — 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 como resultado 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, como la que sigue:

— 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.

Scheme type/community/rules (cláusula 5.3.9)

Este campo DEBERÁ estar presente y cumplir las especificaciones de la cláusula 5.3.9 de TS 119 612, y CONTENDRÁ al menos los siguientes dos URI:

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

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

  Texto descriptivo:

  «*Participation in a scheme*

  Each Member State must create a "Trusted List 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 implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's Trusted List, compiled by the European Commission.

  Policy/rules for the assessment of the listed services

  The Trusted List of a Member State must provide, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 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.

[1] Los dos últimos conjuntos 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 aplicables a los CSP que no expiden QC. Estos conjuntos de información se facilitarán a nivel de la lista de confianza mediante el uso del presente «Scheme information URI» (cláusula 5.3.7 — información facilitada por el Estado miembro), de «Scheme type/community/rules» (cláusula 5.3.9 — mediante el uso de un texto común a todos los Estados miembros) y de «TSL policy/legal notice» (cláusula 5.3.11 — texto común a todos los Estados miembros 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).

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 compliance 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 Article 3(3), Article 8)(1), Article 11 (respectively, Article2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 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 Article 2(11) of Directive 1999/93/EC). 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 Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a Trusted List according to the Annex of Commission Decision [reference to the present Decision] 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 EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no "Sie" "Qualifications Extension" information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related "Sie" "Qualifications Extension" information, 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. QcCompliance, QcSSCD, etc.) 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" "Qualifications Extension" information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this "Sie" "Qualifications Extension" information, 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 the qualified status, the "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 qualified status: "QCStatement" meaning the identified certificate(s) is(are) qualified;

AND/OR

— 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 Member States' Trusted Lists.»

— 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/TrustedList/schemerules/CC donde CC = el código de país ISO 3166-1 ([1]) alfa-2 utilizado en el campo «Scheme territory» (cláusula 5.3.10)

— 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 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» (cláusula 5.5.9).

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

TSL policy/legal notice (cláusula 5.3.11)

Este campo DEBERÁ estar presente y cumplir las especificaciones de la cláusula 5.3.11 de la TS 119 612, y la política o el aviso legal relativos a la situación jurídica del régimen o los requisitos legales que este satisface en la jurisdicción en la que está establecido y/o cualquier restricción o condición bajo la cual se mantenga y publique la lista de confianza SERÁ una cadena de caracteres multilingües (texto sencillo) compuesta por dos partes:

1. Una primera parte obligatoria, común a todas las listas de confianza de los Estados miembros (con el inglés del Reino Unido como lengua obligatoria y, 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 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.

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

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

2. Una segunda parte opcional, específica de cada lista de confianza (con el inglés del Reino Unido como lengua obligatoria y, 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).

CAPÍTULO II

CONTINUIDAD DE LAS LISTAS DE CONFIANZA

Los certificados que deban notificarse a la Comisión de conformidad con el artículo 3, letra c), de la presente Decisión se EXPEDIRÁN de modo que:

— exista, como mínimo, un período de tres meses entre sus fechas de vigencia,

— se creen sobre la base de nuevos pares de claves, puesto que ningún par de claves utilizado previamente deberá certificarse nuevamente.

En caso de que se comprometa o se retire UNA de las claves privadas correspondientes a la clave pública que podría utilizarse para validar la firma de la lista de confianza, y que se haya notificado a la Comisión y figure publicada en las listas centrales de indicadores de la Comisión, los Estados miembros:

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

— NOTIFICARÁN de inmediato a la Comisión la nueva lista de certificados de clave pública correspondientes a las claves privadas que puedan utilizarse para firmar la lista de confianza.

En caso de que se comprometan o se retiren TODAS las claves privadas correspondientes a las claves públicas que podrían utilizarse para validar la firma de la lista de confianza, y que se hayan notificado a la Comisión y figuren publicadas en las listas centrales de indicadores de la Comisión, los Estados miembros:

— GENERARÁN nuevos pares de claves que puedan utilizarse para firmar la lista de confianza y sus certificados de clave pública correspondientes,

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

— NOTIFICARÁN de inmediato a la Comisión la nueva lista de certificados de clave pública correspondientes a las claves privadas que puedan utilizarse para firmar la lista de confianza.

CAPÍTULO III

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

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

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

— la estructura de la forma legible por personas DEBERÍA reflejar el modelo lógico descrito en la TS 119.612.

— DEBERÍAN aparecer 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 (por ejemplo, «una autoridad de certificación que expide certificados de clave pública»),

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

[1] ISO 32000-1:2008: Gestión de documentos — Formato de documento portátil — Parte 1: PDF 1.7
[2] ISO 19005-2:2011: Gestión de documentos — Formato de archivo de documento electrónico para su conservación a largo plazo — Parte 2: Uso de ISO 32000-1 (PDF/A-2).

— DEBERÍAN aparecer como mínimo en la forma legible por personas 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

  — 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 legible por personas DEBERÍA ser fácilmente imprimible.

— La forma legible por personas DEBERÁ ser firmada por el operador del régimen con arreglo al perfil básico de firmas PAdES ([1]).

([1]) ETSI TS 103 172 (marzo de 2012)-Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.