2025/1943

30.9.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/1943 DE LA COMISIÓN

de 29 de septiembre de 2025

por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las normas de referencia para los certificados cualificados de firma electrónica y los certificados cualificados de sello electrónico

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE ([1]), y en particular su artículo 28, apartado 6, y su artículo 38, apartado 6,

Considerando lo siguiente:

(1) Los certificados cualificados de firma electrónica y los certificados cualificados de sello electrónico desempeñan un papel crucial en el entorno empresarial digital al promover la transición de los procesos tradicionales en papel a los procedimientos electrónicos equivalentes. Al vincular los datos de validación de la firma electrónica o del sello electrónico a una persona física o jurídica, respectivamente, y al confirmar el nombre de dicha persona, los certificados cualificados mejoran la seguridad en cuanto a la identidad del firmante y del creador del sello.

(2) La presunción de cumplimiento establecida en el artículo 28, apartado 6, y en el artículo 38, apartado 6, del Reglamento (UE) n.º 910/2014 solo debe aplicarse cuando los servicios de confianza cualificados para la expedición de certificados cualificados de firma electrónica y de certificados cualificados de sello electrónico cumplan las normas establecidas en el presente Reglamento. Estas normas deben reflejar las prácticas establecidas y ser ampliamente aceptadas en los sectores pertinentes. Deben adaptarse para incluir controles adicionales que garanticen la seguridad y la fiabilidad de los servicios de confianza cualificados y del contenido de los certificados cualificados.

(3) Si un prestador de servicios de confianza cumple los requisitos establecidos en el anexo del presente Reglamento, los organismos de supervisión deben presumir el cumplimiento de los requisitos pertinentes del Reglamento (UE) n.º 910/2014 y tener debidamente en cuenta dicha presunción para conceder o confirmar la cualificación del servicio de confianza. No obstante, un prestador cualificado de servicios de confianza puede seguir basándose en otras prácticas para demostrar el cumplimiento de los requisitos del Reglamento (UE) n.º 910/2014.

(4) La Comisión evalúa periódicamente las nuevas tecnologías, prácticas, normas y especificaciones técnicas. De conformidad con el considerando 75 del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo ([2]), la Comisión debe revisar y actualizar el presente Reglamento, en caso necesario, para mantenerlo en consonancia con la evolución mundial, las nuevas tecnologías, normas o especificaciones técnicas y seguir las mejores prácticas del mercado interior.

(5) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([3]) y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([4]) son aplicables a las actividades de tratamiento de datos personales en virtud del presente Reglamento.

([1]) DO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (DO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([5]), emitió su dictamen el 6 de junio de 2025.

(7) Las medidas previstas en el presente Reglamento se ajustan al dictamen del comité establecido por el artículo 48 del Reglamento (UE) n.º 910/2014.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Normas de referencia y especificaciones para los certificados cualificados de firma electrónica y de sello electrónico

1. Las normas de referencia y especificaciones a que se refiere el artículo 28, apartado 6, del Reglamento (UE) n.º 910/2014 figuran en el anexo I del presente Reglamento.

2. Las normas de referencia y especificaciones a que se refiere el artículo 38, apartado 6, del Reglamento (UE) n.º 910/2014 figuran en el anexo II del presente Reglamento.

Artículo 2

Entrada en vigor

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

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

Hecho en Bruselas, el 29 de septiembre de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

([5]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE, (DO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANEXO I

Lista de normas de referencia y especificaciones para los certificados cualificados de firma electrónica

Se aplican las normas ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») y ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5») con las adaptaciones siguientes:

1. En el caso de ETSI EN 319 411-2:

   1) 2.1 Referencias normativas

      — [1] ETSI EN 319 401 V3.1.1 (2024-06) «Firmas electrónicas e infraestructuras de confianza (ESI). Requisitos de política general para proveedores de servicios de confianza».

      — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Firmas electrónicas e infraestructuras de confianza (ESI). Política y requisitos de seguridad para los proveedores de servicios de confianza que emiten certificados. Parte 1: Requisitos generales», con las adaptaciones siguientes:

        La cláusula 2.1 «Referencias normativas» de ETSI EN 319 411-1 V1.5.1 se modifica como sigue:

        — [9] ETSI EN 319 401 V3.1.1 (2024-06) «Firmas electrónicas e infraestructuras de confianza (ESI). Requisitos de política general para proveedores de servicios de confianza».

        — [10] ETSI EN 319 412-2 V2.4.1 «Firmas electrónicas e infraestructuras (ESI). Perfiles de certificados. Parte 2: Perfil de certificado para certificados expedidos a personas físicas».

        — [14] ETSI EN 319 412-1 V1.6.1 «Firmas electrónicas e infraestructuras (ESI). Perfiles de certificados. Parte 1: Visión general y estructuras de datos comunes».

      — [3] ETSI EN 319 412-5 V2.5.1 «Firmas electrónicas e infraestructuras de confianza (ESI). Perfiles de Certificados. Parte 5: Declaraciones de control de calidad».

      — [5] ETSI EN 319 412-1 V1.6.1 «Firmas electrónicas e infraestructuras de confianza (ESI). Perfiles de certificados. Parte 1: Visión general y estructuras de datos comunes».

      — [6] CEN/TS 419261:2015 «Requisitos de seguridad para sistemas de confiabilidad en la gestión de certificados y de sellos de tiempo».

      — [7] Grupo Europeo de Certificación de la Ciberseguridad, Subgrupo de Criptografía: «Agreed Cryptographic Mechanisms» («Mecanismos criptográficos acordados», documento en inglés) publicado por la Agencia de la Unión Europea para la Ciberseguridad («ENISA») ([1]).

      — [8] Reglamento de Ejecución (UE) 2024/482 de la Comisión ([2]), por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo que respecta a la adopción del esquema europeo de certificación de la ciberseguridad basado en criterios comunes (EUCC).

      — [9] Reglamento de Ejecución (UE) 2024/3144 de la Comisión ([3]), por el que se modifica el Reglamento de Ejecución (UE) 2024/482 en lo que respecta a las normas internacionales aplicables y se corrige dicho Reglamento de Ejecución.

      — [10] ISO/IEC 15408:2022 (partes 1 a 5): «Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de TI».

      — [11] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules» («Requisitos de seguridad para módulos criptográficos»)

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) DO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 5.2 Requisitos de la declaración de prácticas de certificación

— OVR-5.2-02 Las políticas de certificación (CP) identificadas por la documentación del prestador de servicios de confianza (TSP) especificarán los requisitos relativos a los perfiles de certificado que deben utilizarse.

3) 5.3 Nombre e identificación de la política de certificación

— OVR-5.3-01 Si se introduce algún cambio en una CP, tal como se describe en la cláusula 4.2.2, que afecte a la aplicabilidad, se modificará el identificador de la política.

4) 6.1 Responsabilidades de publicación y repositorio

— OVR-6.1-02 La información indicada en DIS-6.1-04 de ETSI EN 319 411-1 [2] deberá estar a disposición del público y a escala internacional.

5) 6.2.2 Validación inicial de la identidad

— REG-6.2.2-01A La recopilación de atributos y pruebas sobre la identidad del sujeto, así como su validación, serán las especificadas de conformidad con los actos de ejecución adoptados en virtud del artículo 24, apartado 1 *quater*, del Reglamento (UE) n.º 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] y [QCP-n-qscd] La identidad de la persona física y, en su caso, sus atributos específicos se verificarán de conformidad con los actos de ejecución adoptados en virtud del artículo 24, apartado 1 *quater*, del Reglamento (UE) n.º 910/2014 [i.1].

— NOTA 1: sin efecto.

6) 6.3.3 Expedición de certificados

— GEN-6.3.3-01 Se aplicarán los requisitos GEN-6.3.3-01 a GEN-6.3.3-10 indicados en la norma ETSI EN 319 411-1 [2], cláusula 6.3.3.

— GEN-6.3.3-02 [CONDICIONAL] Si se expide un certificado a una persona física identificada en asociación con la persona jurídica, los atributos del sujeto que identifiquen a la organización en el certificado representarán a la persona jurídica o subentidad de esta y el identificador del sujeto en el certificado será la persona física.

— GEN-6.3.3-03 El identificador de la CP será [ELECCIÓN]:

a) [QCP-n]

— tal como se especifica en la cláusula 5.3, letra a), y/o

— un identificador de objeto (OID), asignado por el TSP, otras partes interesadas pertinentes o una normalización ulterior correspondiente a una política de certificación que mejore los requisitos pertinentes de la política aplicable que se establecen en el presente documento.

b) [QCP-n-qscd]

— tal como se especifica en la cláusula 5.3, letra c), y/o

— un identificador de objeto (OID), asignado por el TSP, otras partes interesadas pertinentes o una normalización ulterior correspondiente a una política de certificación que mejore los requisitos pertinentes de la política aplicable que se establecen en el presente documento.

7) 6.3.5 Uso del par de claves y del certificado

— SDP-6.3.5-02A [CONDICIONAL] Si el TSP gestiona el dispositivo cualificado de creación de firma (QSCD) en nombre del sujeto, el TSP será un prestador cualificado de servicios de confianza que preste un servicio de confianza cualificado para la gestión de un dispositivo cualificado de creación de firma electrónica a distancia, de conformidad con el Reglamento (UE) n.º 910/2014 [i.1].

— SDP-6.3.5-11A Si el suscriptor o el sujeto generan las claves del sujeto, entre las obligaciones del suscriptor (véase la cláusula 6.3.4) figurarán las siguientes:

a) la obligación de generar las claves del sujeto utilizando un algoritmo conforme con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad [7] y publicados por la ENISA para los usos de la clave certificada según se indica en la CP;

b) la obligación de utilizar una longitud de la clave y un algoritmo conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad [7] y publicados por ENISA para los usos de la clave certificada según se indica en la CP durante el período de validez del certificado.

8) 6.3.10 Servicios de estado de los certificados

— CSS-6.3.10-08 [CONDICIONAL] Si se facilitan listas de revocación de certificados (LCR), el TSP preservará la integridad y la disponibilidad de la última LCR al menos durante el período especificado en la declaración de prácticas de certificación (CPS), tal como se exige en CSS-6.3.10-12.

9) 6.4.4 Controles del personal

— OVR-6.4.4-02 El personal del TSP en funciones de confianza y, en su caso, sus subcontratistas en funciones de confianza, deberán ser capaces de cumplir el requisito de poseer los conocimientos especializados, la experiencia y las cualificaciones necesarios obtenidos a través de formación y credenciales formales, o de la experiencia real, o de una combinación de ambas cosas.

— OVR-6.4.4-03 El cumplimiento de los requisitos de OVR-6.4.4-02 incluirá actualizaciones periódicas (al menos cada doce meses) sobre las nuevas amenazas y las prácticas de seguridad actuales.

— OVR-6.4.4-04 Además de las funciones de confianza indicadas en la norma ETSI EN 319 401 [1] (cláusula 7.2-15), se admitirán las funciones de confianza de los funcionarios de registro y revocación con las responsabilidades definidas en la norma TS 419261 [6]. En los casos en que el prestador cualificado de servicios de confianza (QTSP) sea gestionado directamente por un Estado miembro o un organismo del sector público u operado en su nombre, esas funciones de confianza adicionales podrán ser desempeñadas por uno o varios representantes formales que actúen en nombre y por cuenta de los funcionarios de registro y revocación que desempeñan sus funciones en las administraciones locales o regionales.

10) 6.4.9 Cese de la autoridad de certificación (CA) o de la autoridad de registro (RA)

— OVR-6.4.9-02 El plan de cese del TSP cumplirá los requisitos establecidos en los actos de ejecución adoptados en virtud del artículo 24, apartado 5, del Reglamento (UE) n.º 910/2014 [i.1].

11) 6.5.1 Generación e instalación del par de claves

— OVR-6.5.1-01A La generación del par de claves de la CA se llevará a cabo utilizando un algoritmo conforme con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [7] a efectos de firma de la CA.

— OVR-6.5.1-01B La longitud de clave y el algoritmo seleccionados para la clave de firma de la CA serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por la ENISA [7] a efectos de firma de la CA.

— OVR-6.5.1-01C [CONDICIONAL] Si la CA genera las claves del sujeto, las claves del sujeto generadas por esta serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [7] para los fines indicados en la CP durante el período de validez del certificado.

12) 6.5.2 Protección de la clave privada y controles técnicos de los módulos criptográficos

— GEN-6.5.2-01 Serán de aplicación todos los requisitos indicados en ETSI EN 319 411-1 [2], apartado 6.5.2, excepto los requisitos OVR-6.5.2-01, OVR-6.5.2-03 y OVR-6.5.2-04.

— GEN-6.5.2-02 La generación del par de claves del TSP, incluidas las claves utilizadas por los servicios de revocación y registro, se llevará a cabo dentro de un dispositivo criptográfico seguro que sea un sistema fiable certificado de conformidad con:

— los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, tal como se establecen en la norma ISO/IEC 15408 [10] o en los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, versión CC:2002, partes 1 a 5, publicados por los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática, y con certificación EAL 4 o superior; o

— el esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) [8] [9] y con certificación EAL 4 o superior; o

— hasta el 31.12.2030, FIPS PUB 140-3 [11] nivel 3.

Esta certificación se referirá a un objetivo de seguridad o perfil de protección, o a una documentación sobre seguridad y diseño de módulo, que cumpla los requisitos del presente documento, sobre la base de un análisis de riesgos y teniendo en cuenta las medidas de seguridad físicas y otras medidas de seguridad no técnicas.

Si el dispositivo criptográfico seguro cuenta con una certificación EUCC [8][9], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

— GEN-6.5.2-03 La clave de firma privada de la CA se mantendrá y utilizará en un dispositivo criptográfico seguro que cumpla los requisitos de GEN-6.5.2-01 y GEN-6.5.2-02.

13) 6.5.7 Controles de seguridad de la red

— OVR-6.5.7-02 El escaneado de vulnerabilidades exigido en el REQ-7.8-13 de ETSI EN 319 401 [1] se realizará al menos una vez al trimestre.

— OVR-6.5.7-03 La prueba de penetración exigida por REQ-7.8-17X de ETSI EN 319 401 [1] se realizará al menos una vez al año.

— OVR-6.5.7-04 Los cortafuegos estarán configurados de manera que impidan todos los protocolos y accesos que no sean necesarios para el funcionamiento del prestador de servicios de confianza.

14) 6.6.1 Perfil de certificado

— GEN-6.6.1-05 El certificado incluirá uno de los identificadores de política indicados en GEN-6.3.3-03 [ELECCIÓN]. El certificado podrá incluir otros OID asignados por el TSP.

2. En el caso de ETSI EN 319 412-2:

1) 2.1 Referencias normativas

— [2] ETSI EN 319 412-5 V2.5.1 «Firmas electrónicas e infraestructuras de confianza (ESI). Perfiles de Certificados. Parte 5: Declaraciones de control de calidad».

— [9] Grupo Europeo de Certificación de la Ciberseguridad, Subgrupo de Criptografía «Agreed Cryptographic Mechanisms» («Mecanismos criptográficos acordados», documento en inglés) publicado por ENISA.

2) 4.2.2 Firma

— GEN-4.2.2-2 El algoritmo de firma se seleccionará de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [9].

— NOTA: sin efecto.

3) 4.2.3.1 Expedidores que son personas jurídicas

— GEN-4.2.3.1-3 En caso de conocerse la existencia de un número de registro adecuado, la identidad del expedidor contendrá «organizationIdentifier» («identificador de la organización») con un valor de dicho número de registro, tal como conste en el correspondiente registro oficial que determine tal número de registro.

4) 4.2.5 Información sobre la clave pública del sujeto

— GEN-4.2.5-2 La clave pública del sujeto se seleccionará de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [9].

— NOTA: sin efecto.

5) 4.2.6 Número de serie

— GEN-4.2.6-01 El «serialNumber» («número de serie») del certificado (especificado en IETF RFC 5280 [1] cláusula 4.1.2.2) será único para cada certificado expedido por el TSP.

ANEXO II

Lista de normas de referencia y especificaciones para los certificados cualificados de sello electrónico

Se aplican las normas ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-3 V1.3.1 («ETSI EN 319 412-3»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2»), y ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5») con las adaptaciones siguientes:

1. En el caso de ETSI EN 319 411-2:

   1) 2.1 Referencias normativas

      — [1] ETSI EN 319 401 V3.1.1 (2024-06) «Firmas electrónicas e infraestructuras de confianza (ESI). Requisitos de política general para proveedores de servicios de confianza».

      — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Firmas electrónicas e infraestructuras de confianza (ESI). Política y requisitos de seguridad para los proveedores de servicios de confianza que emiten certificados. Parte 1: Requisitos generales», con las adaptaciones siguientes:

        La cláusula 2.1 «Referencias normativas» de ETSI EN 319 411-1 V1.5.1 se modifica como sigue:

        — [9] ETSI EN 319 401 V3.1.1 (2024-06) «Firmas electrónicas e infraestructuras de confianza (ESI). Requisitos de política general para proveedores de servicios de confianza».

        — [10] ETSI EN 319 412-2 V2.4.1 «Firmas electrónicas e infraestructuras (ESI). Perfiles de certificados. Parte 2: Perfil de certificado para certificados expedidos a personas físicas».

        — [14] ETSI EN 319 412-1 V1.6.1 «Firmas electrónicas e infraestructuras (ESI). Perfiles de certificados. Parte 1: Visión general y estructuras de datos comunes».

      — [3] ETSI EN 319 412-5 V2.5.1 «Firmas electrónicas e infraestructuras de confianza (ESI). Perfiles de Certificados. Parte 5: Declaraciones de control de calidad».

      — [5] ETSI EN 319 412-1 V1.6.1 «Firmas electrónicas e infraestructuras de confianza (ESI). Perfiles de certificados. Parte 1: Visión general y estructuras de datos comunes».

      — [6] CEN/TS 419261:2015 «Requisitos de seguridad para sistemas de confiabilidad en la gestión de certificados y de sellos de tiempo» (elaborada por el CEN).

      — [7] Grupo Europeo de Certificación de la Ciberseguridad, Subgrupo de Criptografía: «Agreed Cryptographic Mechanisms» («Mecanismos criptográficos acordados», documento en inglés) publicado por ENISA.

      — [8] Reglamento de Ejecución (UE) 2024/482, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC).

      — [9] Reglamento de Ejecución (UE) 2024/3144, por el que se modifica el Reglamento de Ejecución (UE) 2024/482 en lo que respecta a las normas internacionales aplicables y se corrige dicho Reglamento de Ejecución.

      — [10] ISO/IEC 15408:2022 (partes 1 a 5) «Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de TI».

      — [11] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules» («Requisitos de seguridad para módulos criptográficos»)

   2) 5.2 Requisitos de la declaración de prácticas de certificación

      — OVR-5.2-02 Las políticas de certificación (CP) identificadas por la documentación del prestador de servicios de confianza (TSP) especificarán los requisitos relativos a los perfiles de certificado que deben utilizarse.

3) 5.3 Nombre e identificación de la política de certificación

— OVR-5.3-01 Si se introduce algún cambio en una CP, tal como se describe en la cláusula 4.2.2, que afecte a la aplicabilidad, se modificará el identificador de la política.

4) 6.1 Responsabilidades de publicación y repositorio

— OVR-6.1-02 La información indicada en DIS-6.1-04 de ETSI EN 319 411-1 [2] deberá estar a disposición del público y a escala internacional.

5) 6.2.2 Validación inicial de la identidad

— REG-6.2.2-01A La recopilación de atributos y pruebas sobre la identidad del sujeto, así como su validación, serán las especificadas de conformidad con los actos de ejecución adoptados en virtud del artículo 24, apartado 1 *quater*, del Reglamento (UE) n.º 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] y [QCP-l-qscd] La identidad de la persona jurídica y, en su caso, sus atributos específicos se verificarán de conformidad con los actos de ejecución adoptados en virtud del artículo 24, apartado 1 *quater*, del Reglamento (UE) n.º 910/2014 [i.1].

— NOTA 3: Véase la nota 2.

6) 6.3.3 Expedición de certificados

— GEN-6.3.3-01 Se aplicarán los requisitos GEN-6.3.3-01 a GEN-6.3.3-10 indicados en la norma ETSI EN 319 411-1 [2], cláusula 6.3.3.

— GEN-6.3.3-02 El identificador de la CP será [ELECCIÓN]:

a) [QCP-l]

— según lo especificado en la cláusula 5.3, letra b), y/o

— un identificador de objeto (OID), asignado por el TSP, otras partes interesadas pertinentes o una normalización ulterior correspondiente a una política de certificación que mejore los requisitos pertinentes de la política aplicable que se establecen en el presente documento.

b) [QCP-l-qscd]

— según lo especificado en la cláusula 5.3, letra d), y/o

— un identificador de objeto (OID), asignado por el TSP, otras partes interesadas pertinentes o una normalización ulterior correspondiente a una política de certificación que mejore los requisitos de la política aplicables que se establecen en el presente documento.

7) 6.3.5 Uso del par de claves y del certificado

— SDP-6.3.5-02A [CONDICIONAL] Si el TSP gestiona el dispositivo cualificado de creación de firma electrónica (QSCD) en nombre del sujeto, el TSP será un prestador cualificado de servicios de confianza que preste un servicio de confianza cualificado para la gestión de un dispositivo cualificado de creación de sello electrónico a distancia, de conformidad con el Reglamento (UE) n.º 910/2014 [i.1].

— SDP-6.3.5-11A Si el suscriptor o el sujeto generan las claves del sujeto, entre las obligaciones del suscriptor (véase la cláusula 6.3.4) figurarán las siguientes:

a) la obligación de generar las claves del sujeto utilizando un algoritmo conforme con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por la ENISA [7] para los usos de la clave certificada según se indica en la CP; y

b) la obligación de utilizar una longitud de la clave y un algoritmo conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [7] para los usos de la clave certificada según se indica en la CP durante el período de validez del certificado.

8) 6.3.10 Servicios de estado de los certificados

— CSS-6.3.10-08 [CONDICIONAL] Si se facilitan listas de revocación de certificados (LCR), el TSP preservará la integridad y la disponibilidad de la última LCR al menos durante el período especificado en la declaración de prácticas de certificación (CPS), tal como se exige en CSS-6.3.10-12.

9) 6.4.4 Controles del personal

— OVR-6.4.4-02: El personal del TSP en funciones de confianza y, en su caso, sus subcontratistas en funciones de confianza, deberán ser capaces de cumplir el requisito de poseer los conocimientos especializados, la experiencia y las cualificaciones necesarios obtenidos a través de formación y credenciales formales, o de la experiencia real, o de una combinación de ambas cosas.

— OVR-6.4.4-03 El cumplimiento de los requisitos de OVR-6.4.4-02 incluirá actualizaciones periódicas (al menos cada doce meses) sobre las nuevas amenazas y las prácticas de seguridad actuales.

— OVR-6.4.4-04 Además de las funciones de confianza indicadas en la norma ETSI EN 319 401 [1] (cláusula 7.2-15), se admitirán las funciones de confianza de los funcionarios de registro y revocación con las responsabilidades definidas en la norma TS 419261 [6]. En los casos en que el prestador cualificado de servicios de confianza sea gestionado directamente por un Estado miembro o un organismo del sector público u operado en su nombre, esas funciones de confianza adicionales podrán ser desempeñadas por uno o varios representantes formales que actúen en nombre y por cuenta de los funcionarios de registro y revocación que desempeñan sus funciones en las administraciones locales o regionales.

10) 6.4.9 Cese de la autoridad de certificación (CA) o de la autoridad de registro (RA)

— OVR-6.4.9-02 El plan de cese del TSP cumplirá los requisitos establecidos en los actos de ejecución adoptados en virtud del artículo 24, apartado 5, del Reglamento (UE) n.º 910/2014 [i.1].

11) 6.5.1 Generación e instalación del par de claves

— OVR-6.5.1-01A La generación del par de claves de la CA se llevará a cabo utilizando un algoritmo conforme con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad publicados por ENISA [7] a efectos de firma de la CA.

— OVR-6.5.1-01B La longitud de clave y el algoritmo seleccionados para la clave de firma de la CA serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por la ENISA [7] a efectos de firma de la CA.

— OVR-6.5.1-01C [CONDICIONAL] Si la CA genera las claves del sujeto, las claves del sujeto generadas por esta serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad publicados por ENISA [7] para los fines indicados en la CP durante el período de validez del certificado.

12) 6.5.2 Protección de la clave privada y controles técnicos de los módulos criptográficos

— GEN-6.5.2-01 Serán de aplicación todos los requisitos indicados en ETSI EN 319 411-1 [2], apartado 6.5.2, excepto los requisitos OVR-6.5.2-01, OVR-6.5.2-03 y OVR-6.5.2-04.

— GEN-6.5.2-02 La generación del par de claves del TSP, incluidas las claves utilizadas por los servicios de revocación y registro, se llevará a cabo dentro de un dispositivo criptográfico seguro que sea un sistema fiable certificado de conformidad con:

  — los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, tal como se establecen en la norma ISO/IEC 15408 [10] o en los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, versión CC:2002, partes 1 a 5, publicados por los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática, y con certificación EAL 4 o superior; o

  — el esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) [8] [9] y con certificación EAL 4 o superior; o

  — hasta el 31.12.2030, FIPS PUB 140-3 [11] nivel 3.

Esta certificación se referirá a un objetivo de seguridad o perfil de protección, o a una documentación sobre seguridad y diseño de módulo, que cumpla los requisitos del presente documento, sobre la base de un análisis de riesgos y teniendo en cuenta las medidas de seguridad físicas y otras medidas de seguridad no técnicas.

Si el dispositivo criptográfico seguro cuenta con una certificación EUCC [8] [9], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

— GEN-6.5.2-03 La clave de firma privada de la CA se mantendrá y utilizará en un dispositivo criptográfico seguro que cumpla los requisitos de GEN-6.5.2-01 y GEN-6.5.2-02.

13) 6.5.7 Controles de seguridad de la red

— OVR-6.5.7-02 El escaneado de vulnerabilidades exigido en el REQ-7.8-13 de ETSI EN 319 401 [1] se realizará al menos una vez al trimestre.

— OVR-6.5.7-03 La prueba de penetración exigida por REQ-7.8-17X de ETSI EN 319 401 [1] se realizará al menos una vez al año.

— OVR-6.5.7-04 Los cortafuegos estarán configurados de manera que impidan todos los protocolos y accesos que no sean necesarios para el funcionamiento del prestador de servicios de confianza.

14) 6.6.1 Perfil de certificado

— GEN-6.6.1-05 El certificado incluirá uno de los identificadores de política indicados en GEN-6.3.3-02 [ELECCIÓN].

2. En el caso de ETSI EN 319 412-3:

1) 2.1 Referencias normativas

— [2] ETSI EN 319 412-2 V2.4.1 «Firmas electrónicas e infraestructuras de confianza (ESI). Perfiles de certificados. Parte 2: Perfil de certificado para certificados expedidos a personas físicas».

2) 4.2.1 Sujeto

— LEG-4.2.1-6 El atributo «organizationIdentifier» («identificador de la organización») contendrá una identificación de la organización sujeto distinta del nombre de la organización. En caso de conocerse la existencia de un número de registro adecuado, el atributo «organizationIdentifier» contendrá un valor de dicho número de registro, tal como conste en el correspondiente registro oficial que determine tal número de registro.

3. En el caso de ETSI EN 319 412-2:

1) 2.1 Referencias normativas

— [2] ETSI EN 319 412-5 V2.5.1 «Firmas electrónicas e infraestructuras de confianza (ESI). Perfiles de Certificados. Parte 5: Declaraciones de control de calidad».

— [9] Grupo Europeo de Certificación de la Ciberseguridad, Subgrupo de Criptografía: «Agreed Cryptographic Mechanisms» («Mecanismos criptográficos acordados», documento en inglés) publicado por ENISA.

2) 2.2 Referencias informativas

— [i.7] sin efecto.

3) 4.2.2 Firma

— GEN-4.2.2-2 El algoritmo de firma se seleccionará de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [9].

— NOTA: sin efecto.

4) 4.2.3.1 Expedidores que son personas jurídicas

— GEN-4.2.3.1-3 En caso de conocerse la existencia de un número de registro adecuado, la identidad del expedidor contendrá «organizationIdentifier» («identificador de la organización») con un valor de dicho número de registro, tal como conste en el correspondiente registro oficial que determine tal número de registro.

5) 4.2.5 Información sobre la clave pública del sujeto

— GEN-4.2.5-2 La clave pública del sujeto se seleccionará de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [9].

— NOTA: sin efecto.

6) 4.2.6 Número de serie

— GEN-4.2.6-01 El «serialNumber» («número de serie») del certificado (especificado en IETF RFC 5280 [1] cláusula 4.1.2.2) será único para cada certificado expedido por el TSP.