2025/1942

30.9.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/1942 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 los servicios cualificados de validación de firmas electrónicas cualificadas y los servicios cualificados de validación de sellos electrónicos cualificados

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 33, apartado 2, y su artículo 40,

Considerando lo siguiente:

(1) Los servicios cualificados de validación de firmas electrónicas cualificadas y de sellos electrónicos cualificados garantizan la integridad, la autenticidad, y la corrección del proceso y los resultados de la validación de las firmas electrónicas cualificadas y de los sellos electrónicos cualificados, respectivamente. Tales servicios de confianza cualificados desempeñan un papel crucial en el entorno empresarial digital al promover la transición de los procesos tradicionales en papel a los procedimientos electrónicos equivalentes.

(2) La presunción de cumplimiento establecida en el artículo 33, apartado 2, y el artículo 40 del Reglamento (UE) n.º 910/2014 solo debe aplicarse cuando los servicios cualificados de validación de firmas electrónicas cualificadas y de sellos electrónicos cualificados cumplan las normas técnicas 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, así como la capacidad de verificar la cualificación y la validez técnica de las firmas electrónicas cualificadas y los sellos electrónicos 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.

([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).

(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.

(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

En el anexo del presente Reglamento se establecen las normas de referencia y las especificaciones a que se refieren el artículo 33, apartado 2, y el artículo 40 del Reglamento (UE) n.º 910/2014.

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

([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).

([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

Lista de normas de referencia y especificaciones para servicios cualificados de validación de firmas electrónicas cualificadas y para servicios cualificados de validación de sellos electrónicos cualificados

Se aplican las normas ETSI TS 119 441 V1.2.1 (2023-10) ([1]) («ETSI TS 119 441») y ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) («ETSI TS 119 172-4») con las siguientes adaptaciones:

1. En el caso de ETSI TS 119 441

1) 2.1 Referencias normativas

— [1] ETSI TS 119 101 V1.1.1 (2016-03) «Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation» [«Firmas electrónicas e infraestructuras (ESI). Requisitos de política y seguridad para las solicitudes de creación y validación de firmas»].

— [2] 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».

— [3] ETSI EN 319 102-1 V1.4.1 (2024-06) «Firmas electrónicas e infraestructuras de confianza (ESI). Procedimientos para la creación y validación de firmas digitales AdES. Parte 1: Creación y validación».

— [4] ISO/IEC 15408-1:2022 «Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de TI».

— [5] sin efecto.

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

— [7] Reglamento de Ejecución (UE) 2024/482 de la Comisión ([3]), 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).

— [8] ETSI TS 119 172-4 V1.1.1 (2021-05) «Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists» [«Firmas electrónicas e infraestructuras (ESI). Políticas de firma. Parte 4: Normas de aplicabilidad de la firma (política de validación) para firmas/sellos electrónicos cualificados europeos que utilizan listas de confianza»].

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) «Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report» [«Firmas electrónicas e infraestructuras de confianza (ESI). Procedimientos para la creación y validación de firmas digitales AdES. Parte 2: Informe de validación de firmas»].

— [10] 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») ([4]).

— [11] Reglamento de Ejecución (UE) 2024/3144 de la Comisión ([5]), por el que se modifica el Reglamento de Ejecución (UE) 2024/4822 en lo que respecta a las normas internacionales aplicables y se corrige dicho Reglamento de Ejecución.

— [12] ETSI EN 319 411-1 «Firmas electrónicas e infraestructuras (ESI). Política y requisitos de seguridad para los proveedores de servicios de confianza que emiten certificados. Parte 1: Requisitos generales».

([1]) ETSI TS 119 441: «Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services» [«Firmas electrónicas e infraestructuras (ESI). Requisitos de política para TSP que presten servicios de validación de firmas»], V1.2.1 (2023-10).

([2]) ETSI TS 119 172-4: «Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists» [«Firmas electrónicas e infraestructuras (ESI). Políticas de firma. Parte 4: Normas de aplicabilidad de la firma (política de validación) para firmas/sellos electrónicos cualificados europeos que utilizan listas de confianza»], V1.1.1 (2021-05).

([3]) DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

([5]) DO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Referencias informativas

— [i.11] sin efecto.

3) 3.3 Siglas

— EUCC Esquema europeo de certificación de la ciberseguridad basado en los criterios comunes

4) 4.3.3 Proceso

— NOTA 10 Véase ETSI EN 319 102-1 [3] para obtener orientación y ETSI TS 119 172-4 [8] a fin de obtener orientaciones adicionales para el caso de firma o sello cualificado de la UE.

5) 6.1 Declaración de prácticas del servicio de validación de firmas

— OVR-6.1-02 La declaración de prácticas del SVS (servicio de validación de firmas) se estructurará con arreglo al anexo A.

— OVR-6.1-03 La declaración de prácticas del SVS enumerará o hará referencia a las políticas del SVS admitidas (por ejemplo, a través de identificadores de objeto) y las describirá brevemente.

6) 6.3 Política de seguridad de la información

— OVR-6.3-02 La política de seguridad documentará los controles de seguridad y privacidad aplicados para proteger los datos personales.

7) 7.2 Recursos humanos

— OVR-7.2-02 El personal del prestador de servicio de validación de firmas (SVSP) 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-7.2-03 El cumplimiento de los requisitos de OVR-7.2-02 incluirá actualizaciones periódicas (al menos cada doce meses) sobre las nuevas amenazas y las prácticas de seguridad actuales.

8) 7.5 Controles criptográficos

— OVR-7.5-02 [CONDICIONAL] Cuando se firmen los informes de validación, una CA fiable expedirá el certificado de firma pública del SVSP correspondiente a la clave de firma privada del SVSP, de conformidad con la política de certificación NCP+ especificada en la norma ETSI EN 319 411-1 [12]. Debe expedirse de conformidad con una política de certificación adecuada especificada en la norma ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDICIONAL] Cuando se firmen informes de validación, la clave de firma privada del SVSP se custodiará y utilizará en un dispositivo criptográfico seguro que sea un sistema fiable certificado de conformidad con:

a) 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 [4] o en los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, versión CC:2022, 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

b) EUCC [7][11] y con certificación EAL 4 o superior, o

c) hasta el 31.12.2030, FIPS PUB 140-3 [6] 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 [7] [11], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

— OVR-7.5-04 sin efecto.

— OVR-7.5-06 Una clave de firma privada de SVSP solo se exportará e importará a un dispositivo criptográfico seguro diferente cuando dicha exportación e importación se lleven a cabo de forma segura y de conformidad con la certificación de dichos dispositivos.

9) 7.7 Seguridad del funcionamiento

— OVR-7.7-02 A fin de garantizar que los sistemas en los que se desarrolla la aplicación aplican medidas de seguridad adecuadas y se adaptan a entornos de aplicación específicos, la SVA (aplicación de validación de firmas) utilizará un entorno de aplicación que esté recibiendo mantenimiento con correcciones de seguridad actualizadas.

— OVR-7.7-03 Se aplicarán a la SVA los siguientes requisitos que se especifican en ETSI TS 119 101 [1], cláusula 5.2: GSM 1.3.

10) 7.8 Seguridad de la red

— OVR-7.8-02 Si se permite el acceso a distancia a sistemas que almacenan o tratan datos confidenciales, se adoptará una política formal, que se describirá como parte de los elementos exigidos por OVR-6.3-02.

— OVR-7.8-04 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-7.8-05 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-7.8-06 Los cortafuegos estarán configurados de manera que impidan todos los protocolos y accesos que no sean necesarios para el funcionamiento del SVSP.

11) 7.12 Cese de la prestación del servicio de validación de firmas y planes de cese

— OVR-7.12-02 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].

12) 7.14 Cadena de suministro

— OVR-7.14-01 Se aplicarán los requisitos especificados en la norma ETSI EN 319 401 [2], cláusula 7.14.

13) 8.1 Proceso de validación de firmas

— VPR-8.1-07 La aplicación de validación (SVA) cumplirá los requisitos de ETSI TS 119 101 [1], cláusula 7.4 SIA 1 a SIA 4.

— VPR-8.1-11 [CONDICIONAL] Cuando el SVS tenga por objeto validar firmas electrónicas cualificadas o sellos electrónicos cualificados, de conformidad con el artículo 32, apartado 1, (o el artículo 40, respectivamente) del Reglamento (UE) n.º 910/2014 [i.1], el proceso de validación se ajustará a los requisitos de ETSI TS 119 172-4 [8].

14) 8.2 Protocolo de validación de firmas

— SVP-8.2-03 La respuesta de validación de la firma llevará el identificador de objeto (OID(de la política del SVS.

15) 8.4 Informe de validación de firmas

— SVR-8.4-02 El informe de validación se ajustará a ETSI TS 119 102-2 [9].

— SVR-8.4-07 [CONDICIONAL] Cuando el SVS no procese completamente una política de validación de firmas, el informe, además de informar sobre las limitaciones validadas, comunicará las limitaciones que hayan sido ignoradas o anuladas.

— SVR-8.4-15 El informe de validación indicará claramente el origen de cada PoE (prueba de existencia) —desde el interior de la firma, desde el cliente o desde el servidor).

— SVR-8.4-16 El informe de validación llevará una firma de informe de validación, que será la firma digital del SVSP.

— SVR-8.4-17 [CONDICIONAL] Cuando se firmen los informes de validación, el formato y el objetivo de la firma se ajustarán a ETSI TS 119 102-2 [9].

16) 9 Marco para la definición de políticas de servicios de validación basadas en una política de servicios de confianza definida en el presente documento:

— OVR-9-05 [CONDICIONAL] Al elaborar una política de SVS sobre una política de servicios de confianza definida en el presente documento, se llevará a cabo una evaluación de riesgos a fin de evaluar los requisitos operativos y determinar los requisitos de seguridad que deben incluirse en la política para la aplicabilidad y comunidad declaradas.

— OVR-9-06 [CONDICIONAL] Al elaborar una política de SVS sobre una política de servicios de confianza definida en el presente documento, la política se aprobará y modificará de conformidad con un proceso de revisión definido, incluidas las responsabilidades relativas al mantenimiento de la política.

— OVR-9-07 [CONDICIONAL] Al elaborar una política de SVS sobre una política de servicios de confianza definida en el presente documento, deberá existir un proceso de revisión definido a fin de garantizar que la política esté admitida por las declaraciones prácticas.

— OVR-9-08 [CONDICIONAL] Al elaborar una política de SVS sobre una política de servicios de confianza definida en el presente documento, el TSP facilitará a su comunidad de usuarios las políticas que admite.

— OVR-9-09 [CONDICIONAL] Al elaborar una política de SVS sobre una política de servicios de confianza definida en el presente documento, se facilitarán a los suscriptores las revisiones de las políticas admitidas por el TSP.

17) Anexo B (normativo) Servicio cualificado de conservación de firmas electrónicas cualificadas (QES), tal como se establece en el artículo 33 del Reglamento (UE) n.º 910/2014:

— VPR-B-02 [CONDICIONAL] Si el SVSP es un prestador cualificado de servicio de validación de firmas (QSVSP), la implementación deberá cumplir lo dispuesto en ETSI TS 119 172-4 [8].

— NOTA 2 sin efecto.

— OVR-B-04 [CONDICIONAL] Si el SVSP es un QSVSP, los ensayos de OVR-B-03 comprobarán diferentes casos de uso, positivos y negativos.

— VPR-B-11 [CONDICIONAL] Si el SVSP es un QSVSP, el SVSP controlará el cálculo del *hash* (ya sea efectuando el cálculo en el lado del servidor o controlando al cliente si está permitido en el lado del cliente).

— NOTA 5 sin efecto.

— NOTA 6 sin efecto.

— VPR-B-15 [CONDICIONAL] Si el SVSP es un QSVSP, a fin de cumplir lo dispuesto en VPR-B-13 a VPR-B-14 el informe de validación será conforme con ETSI TS 119 102-2 [9].

— VPR-B-16 [CONDICIONAL] Si el SVSP es un QSVSP, la aplicación se ajustará a los mecanismos criptográficos acordados publicados por el Grupo Europeo de Certificación de la Ciberseguridad de ENISA [10] para el uso de técnicas criptográficas adecuadas a la hora de prestar servicios cualificados de validación para firmas electrónicas cualificadas.

18) Anexo C (informativo) Correlación de los requisitos del Reglamento (UE) n.º 910/2014, sección relativa a la realización de la validación de conformidad con el artículo 32, apartado 1, párrafo segundo:

— A fin de garantizar que se verifiquen todas las condiciones exigidas por el artículo 32, apartado 1, y el artículo 40 del Reglamento (UE) n.º 910/2014 [i.40], es necesario un algoritmo de validación correcto. Proporciona el mismo resultado determinista para una firma o sello presentado para su validación. La política de validación de firmas es crucial para este fin. Se ha publicado con esta perspectiva la norma ETSI TS 119 172-4 [8], basada en el algoritmo de validación especificado en la norma ETSI EN 319 102-1 [3].

2. En el caso de ETSI TS 119 172-4

1) 2.1 Referencias normativas

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) «Firmas electrónicas e infraestructuras de confianza (ESI). Procedimientos para la creación y validación de firmas digitales AdES. Parte 1: Creación y validación».

— Todas las referencias a «ETSI TS 119 102-1 [1]» se entenderán hechas a «ETSI EN 319 102-1 [1]».

— [2] ETSI TS 119 612 V2.3.1 (2024-11) «Electronic Signatures and Infrastructures (ESI); Trusted Lists» [«Firmas electrónicas e infraestructuras (ESI). Listas de confianza»].

— [13] ETSI TS 119 101 V1.1.1 (2016-03) «Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation» [«Firmas electrónicas e infraestructuras (ESI). Requisitos de política y seguridad para las solicitudes de creación y validación de firmas»].

2) 4.2 Restricciones para la validación y procedimientos de validación, requisito REQ-4.2-03, sección «Restricciones para la validación X.509», letra c):

— i) Si un certificado de entidad final representa un ancla de confianza, no se utilizarán las «RevocationCheckingConstraints» («restricciones relativas a la comprobación de la revocación»).

— ii) Si un certificado de entidad final no representa un ancla de confianza, las «RevocationCheckingConstraints» se establecerán en «eitherCheck» («cualquier comprobación»), según se define en ETSI TS 119 172-1 [3], cláusula A.4.2.1, cuadro A.2, filas (m)2.1.

— iii) Si un certificado de entidad final representa un ancla de confianza, no se utilizarán las «RevocationFreshnessConstraints» («restricciones relativas a la actualidad de la revocación») definidas en ETSI TS 119 172-1 [3], cláusula A.4.2.1, cuadro A.2, filas (m)2.2.

— iv) Si un certificado de entidad final no representa un ancla de confianza, se utilizarán las «RevocationFreshnessConstraints» definidas en ETSI TS 119 172-1 [3], cláusula A.4.2.1, cuadro A.2, filas (m)2.2, con un valor máximo de 24 horas para el certificado de firma. No se fijará ningún valor para las «RevocationFreshnessConstraints» para los certificados distintos del certificado de firma, incluidos los certificados que admitan sellos de tiempo.

3) 4.4 Proceso de comprobación de (las normas de) la aplicabilidad técnica

— REQ-4.4.2-03 Si alguno de los controles especificados en REQ-4.4.2-01 no es conforme, entonces:

a) el proceso se detiene;

b) la firma se considerará técnicamente como indeterminada, es decir, no como una firma electrónica cualificada de la UE ni como un sello electrónico cualificado de la UE;

c) el resultado mencionado y los resultados de los procesos de todos los procesos intermedios se reflejarán en el informe de comprobación de las normas de la aplicabilidad de la firma.