2025/1946

30.9.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/1946 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 conservación de firmas electrónicas cualificadas y 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 34, apartado 2, y su artículo 40,

Considerando lo siguiente:

(1) Los servicios cualificados de conservación de firmas electrónicas cualificadas y de sellos electrónicos cualificados garantizan a largo plazo la integridad, la autenticidad, la prueba de la existencia y la accesibilidad de las pruebas de conservación de dichas firmas electrónicas y de sellos electrónicos. Esto permite demostrar su validez jurídica durante períodos de tiempo prolongados y garantiza que puedan validarse con independencia de los futuros cambios tecnológicos. Estos servicios se prestan de forma independiente o como parte de otro servicio de confianza cualificado, como los servicios cualificados de archivo electrónico.

(2) La presunción de cumplimiento establecida en el artículo 34, apartado 1 *bis*, y el artículo 40 del Reglamento (UE) n.º 910/2014 solo debe aplicarse cuando los servicios cualificados de conservación de firmas electrónicas cualificadas y de sellos electrónicos cualificados 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 del servicio de confianza cualificado, así como la capacidad de verificar la cualificación y la validez técnica de las firmas y los sellos a lo largo del tiempo.

(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 34, 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 y especificaciones de referencia a que se refiere el artículo 2

Se aplican las normas ETSI TS 119 511 V1.1.1 (2019-06) («ETSI TS 119 511») y ETSI TS 119 172-4 V1.1.1 (2021-05) («ETSI TS 119 172-4») con las siguientes adaptaciones:

1. En el caso de ETSI TS 119 511

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

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

— [6] Reglamento de Ejecución (UE) 2024/482 de la Comisión ([1]) 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).

— [7] Reglamento de Ejecución (UE) 2024/3144 de la Comisión ([2]) 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.

— [8] 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») ([3]).

— [9] 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»].

— [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».

2) 3.1 Términos

— dispositivo criptográfico seguro: dispositivo que custodia la clave privada del usuario, la protege de ser puesta en peligro y realiza funciones de firma o descifrado en nombre del usuario.

3) 6.4 Perfiles de conservación

— OVR-6.4-08A [WTS][WOS] La duración prevista de las pruebas será conforme con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA 3 sin efecto.

4) 6.5 Política de conservación de pruebas

— OVR-6.5-04A Los algoritmos criptográficos utilizados serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA 1 sin efecto.

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

5) 7.2 Recursos humanos

— OVR-7.2-02 El personal del prestador de servicios de conservación (PSP) 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.

6) 7.5 Controles criptográficos

— OVR-7.5-05 [CONDICIONAL] Cuando el PSP firme (parte de) una prueba de conservación, la clave de firma privada del PSP 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 [10] 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 [6][7] y con certificación EAL 4 o superior; o

c) hasta el 31.12.2030, FIPS PUB 140-3 [5] 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 [6][7], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

— OVR-7.5-06 [CONDICIONAL] sin efecto.

— OVR-7.5-07 [CONDICIONAL] Cuando el PSP firme (parte de) una prueba de conservación, las copias de seguridad de las claves de firma privadas del PSP estarán protegidas para garantizar su integridad y confidencialidad mediante el dispositivo criptográfico seguro antes de almacenarse fuera de dicho dispositivo.

— OVR-7.5-08 Una clave de firma privada de PSP 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.

7) 7.8 Seguridad de la red

— OVR-7.8-03 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-7.8-04 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-7.8-05 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.

8) 7.14 Supervisión criptográfica

— OVR-7.14-03A La evaluación de los algoritmos criptográficos de OVR-7.14.01 y OVR-7.14.02 serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA sin efecto.

9) 7.12 Cese y planes de cese del TSP

— OVR-7.12-01A 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.2].

10) 7.17 Cadena de suministro

— OVR-7.17-01 Se aplicarán los requisitos especificados en la norma ETSI EN 319 401 [1], cláusula 7.14.

11) Anexo A (normativo): Servicio cualificado de conservación de firmas electrónicas cualificadas (QES), tal como se establece en el artículo 34 del Reglamento (UE) n.º 910/2014

— OVR-A-02 [PDS][PDS+PGD]

a) el servicio de conservación conservará toda la información necesaria para comprobar la cualificación de la firma o el sello electrónicos que no estaría a disposición del público hasta el final del período de conservación;

b) el servicio de conservación garantizará que, en cualquier momento durante el período de conservación, la información conservada sea tal que, cuando se facilite como entrada en el proceso especificado en la cláusula 4.4 de ETSI TS 119 172-4 [9], el resultado de este proceso determine claramente si la firma o el sello digitales, en el momento de su conservación, eran técnicamente adecuados para implementar una firma electrónica cualificada de la UE o un sello electrónico cualificado de la UE.

— OVR-A-03 [PDS][PDS+PGD] Los sellos temporales utilizados en las pruebas de conservación serán sellos temporales cualificados de conformidad con el Reglamento (UE) n.º 910/2014 [i.2].

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) «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 0 para el certificado de firma, garantizando que la información sobre revocación solo se acepte si ha sido emitida después del mejor tiempo de la 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) 4.3 Requisitos relativos a la validación de la firma y prácticas de comprobación de las normas de aplicabilidad

— REQ-4.3-02 Las aplicaciones de validación de firmas deberán ser conformes con ETSI TS 119 101 [13].

4) 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:

— el proceso se detiene;

— 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;

— 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.