2025/1944

30.9.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/1944 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 de los procesos de envío y recepción de datos en los servicios cualificados de entrega electrónica certificada y en lo que respecta a la interoperabilidad de tales servicios

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 44, apartados 2 y 2 *ter*,

Considerando lo siguiente:

(1) Los servicios cualificados de entrega electrónica certificada proporcionan un canal seguro para la transmisión de documentos, incluida la prueba del envío y la recepción de los datos. Su objetivo es proporcionar seguridad a la hora de identificar al destinatario y garantizar un alto nivel de confianza en la identificación del remitente.

(2) La presunción de cumplimiento establecida en el artículo 44, apartado 1 *bis*, del Reglamento (UE) n.º 910/2014 solo debe aplicarse cuando los servicios de confianza cualificados para la prestación de servicios cualificados de entrega electrónica certificada 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.

(3) Si un prestador de servicios de confianza cumple los requisitos establecidos en el anexo I 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) De conformidad con el artículo 44, apartado 2 *bis*, del Reglamento (UE) n.º 910/2014, cuando los prestadores cualificados de servicios de confianza acuerden que sus servicios sean interoperables, es importante que cumplan las normas y especificaciones adecuadas establecidas en el anexo II del presente Reglamento de Ejecución a fin de transferir fácilmente los datos electrónicos registrados entre dos o más prestadores cualificados de servicios de confianza y promover prácticas justas en el mercado interior.

(5) 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).

(6) 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 todas las actividades de tratamiento de datos personales en virtud del presente Reglamento.

(7) 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.

(8) 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 servicios cualificados de entrega electrónica certificada

Las normas y especificaciones de referencia a que se refiere el artículo 44, apartado 2, del Reglamento (UE) n.º 910/2014 figuran en el anexo I del presente Reglamento.

Artículo 2

Normas de referencia y especificaciones para la interoperabilidad entre los servicios cualificados de entrega electrónica certificada

Las normas y especificaciones de referencia a que se refiere el artículo 44, apartado 2 *ter*, del Reglamento (UE) n.º 910/2014 figuran en el anexo II del presente Reglamento.

Artículo 3

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 I

Lista de normas y especificaciones de referencia a que se refiere el artículo 1

Se aplica la norma ETSI EN 319 521 V1.1.1 (2019-02) («ETSI EN 319 521») aplica con las siguientes adaptaciones:

1. En el caso de ETSI EN 319 521

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 (ESI). Política y requisitos de seguridad para los proveedores de servicios de confianza que emiten certificados. Parte 1: Requisitos generales».

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) «Firmas electrónicas e infraestructuras (ESI). Servicios de entrega electrónica registrada. Parte 1: Marco y arquitectura».

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) «Firmas electrónicas e infraestructuras (ESI). Servicios de entrega electrónica registrada. Parte 2: Contenidos semánticos».

— [5] 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]).

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

— [7] 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).

— [8] 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.

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

2) 3.1 Términos

— sello electrónico avanzado: según se define en el Reglamento (UE) n.º 910/2014 [i.1].

— firma electrónica avanzada: según se define en el Reglamento (UE) n.º 910/2014 [i.1].

— sello electrónico cualificado: según se define en el Reglamento (UE) n.º 910/2014 [i.1].

— firma electrónica cualificada: según se define en el Reglamento (UE) n.º 910/2014 [i.1].

— 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.

([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.

3) 5.1.1 Disposiciones comunes

— REQ-ERDS-5.1.1-01 El ERDS (servicio de entrega electrónica certificada) velará por que se garanticen adecuadamente la disponibilidad, integridad y confidencialidad del contenido del usuario mientras sea gestionado por el ERDS, seleccionando técnicas criptográficas adecuadas de integridad y confidencialidad conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [5].

4) 5.2.1.1 Generalidades

— REQ-QERDS-5.2.1.1-01 El prestador de servicio cualificado de entrega electrónica certificada (QERDSP) verificará con un nivel de confianza muy elevado la identidad del destinatario, ya sea directamente o recurriendo a un tercero, y utilizando uno de los siguientes medios o una combinación de los mismos, según sea necesario:

a) a través de la presencia física de la persona física o de un representante autorizado de la persona jurídica, mediante pruebas y procedimientos adecuados, de conformidad con el Derecho nacional;

b) a distancia, utilizando un medio de identificación electrónica que cumpla los requisitos establecidos en el artículo 8 del Reglamento (UE) n.º 910/2014 [i.1] con respecto al nivel de seguridad alto, o a través de la cartera europea de identidad digital;

c) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado;

d) utilizando otros métodos de identificación que garanticen que la persona física o el representante autorizado de la persona jurídica pueda ser identificado con un nivel de confianza muy elevado. Un organismo de evaluación de la conformidad confirmará la garantía de que esta identificación se lleva a cabo con un nivel de confianza muy elevado.

— REQ-QERDS-5.2.1.1-01A El QERDSP verificará la identidad del remitente por los medios adecuados, ya sea directamente o recurriendo a un tercero, sobre la base de uno de los métodos siguientes o de una combinación de los mismos:

a) a través de la presencia física de la persona física o de un representante autorizado de la persona jurídica, mediante pruebas y procedimientos adecuados, de conformidad con el Derecho nacional;

b) a distancia, por medio de la cartera europea de identidad digital o de un medio de identificación electrónica notificado que cumpla los requisitos establecidos en el artículo 8 del Reglamento (UE) n.º 910/2014 [i.1] en lo que respecta al nivel de seguridad «sustancial», siempre que se haya expedido sobre la base de la presencia física previa de la persona física o de un representante autorizado de la persona jurídica;

c) mediante un certificado de firma electrónica avanzada o de sello electrónico avanzado, siempre que el certificado se haya expedido a la persona física o a un representante autorizado de la persona jurídica con arreglo a la política de certificación normalizada (NCP) definida en la norma ETSI EN 319 411-1 [2]; o

d) utilizando otros métodos de identificación que garanticen que la persona física o el representante autorizado de la persona jurídica pueda ser identificado con un nivel de confianza muy elevado. Un organismo de evaluación de la conformidad confirmará la garantía de que esta identificación se lleva a cabo con un nivel de confianza elevado.

— NOTA El tercero que verifique la identidad del remitente y del destinatario podrá ser otro QERDSP si el remitente y el destinatario están suscritos a diferentes QERDSP.

5) 5.2.1.2 Identificación del destinatario y entrega del contenido del usuario

— REQ-QERDS-5.2.1.2-03 Si la identificación del destinatario se basa en un proceso interno del QERDS, el QERDSP llevará a cabo todo el proceso en un entorno seguro y controlado.

6) 5.2.2 Disposiciones para la autenticación de QERDS de la UE

— REQ-QERDS-5.2.2-03 [CONDICIONAL] Cuando el QERDSP vincule medios de autenticación con una identidad de remitente verificada con arreglo a la cláusula 5.2.1, serán uno de los siguientes:

a) mecanismos de autenticación de dos factores;

b) la cartera europea de identidad digital o de un medio de identificación electrónica notificado que satisfaga los requisitos establecidos en el artículo 8 del Reglamento (UE) n.º 910/2014 [i.1] con respecto al nivel de seguridad «alto» o «sustancial»;

c) una autenticación TLS mutua que incluya el certificado expedido al remitente con arreglo a la NCP definida en la norma ETSI EN 319 411-1 [2];

d) una firma digital respaldada por un certificado expedido con arreglo a la NCP definida en la norma ETSI EN 319 411-1 [2];

e) otros medios que garanticen la autenticación del remitente identificado. La conformidad de la vinculación será confirmada por un organismo de evaluación de la conformidad. Ejemplo: Esto puede incluir el uso de uno de los medios anteriores de las letras a), b) y d) para registrar un certificado de cliente de seguridad de la capa de transporte (TLS) para el envío automatizado a través de TLS mutua, o para registrar un certificado de sello digital utilizado para sellar manifestaciones a fin de autenticar con el ERDS. También pueden aplicarse otros mecanismos en los que los remitentes identificados recurren a servicios delegados de terceros.

— REQ-QERDS-5.2.2-03A [CONDICIONAL] Cuando el QERDSP vincule medios de autenticación con una identidad de destinatario verificada con arreglo a la cláusula 5.2.1, serán uno de los siguientes, siempre que los medios, o cualquier combinación de ellos, garanticen un nivel de confianza muy elevado en relación con la identidad del destinatario autenticado:

a) un mecanismo de autenticación multifactor;

b) la cartera europea de identidad digital o de un medio de identificación electrónica notificado que satisfaga los requisitos establecidos en el artículo 8 del Reglamento (UE) n.º 910/2014 [i.1] con respecto al nivel de seguridad «alto» o «sustancial»;

c) un certificado de una firma electrónica cualificada o de un sello electrónico cualificado;

d) otros medios que garanticen la autenticación del destinatario identificado. La conformidad de la vinculación será confirmada por un organismo de evaluación de la conformidad. Ejemplo: Esto puede incluir el uso de uno de los medios anteriores de las letras a) a c) para registrar un certificado de cliente de seguridad de la capa de transporte (TLS) para el envío automatizado a través de TLS mutua, o para registrar un certificado de sello digital utilizado para sellar manifestaciones a fin de autenticar con el ERDS. También pueden aplicarse otros mecanismos en los que los remitentes identificados recurren a servicios delegados de terceros.

— REQ-QERDS-5.2.2-04 [CONDICIONAL] Si el remitente se conecta al QERDS en una conexión segura que requiere una autenticación mutua de máquina a máquina entre la máquina del remitente y el servidor del QERDS sobre la base de certificados expedidos con arreglo a la política NCP definida en la norma ETSI EN 319 411-1 [2], una vez establecida esta conexión segura, podrán adoptarse mecanismos de autenticación de un solo factor para una segunda fase de autenticación del remitente si los procedimientos organizativos y las medidas de seguridad implantados garantizan la confianza en la autenticación del remitente.

7) 5.4.1 Disposiciones comunes

— REQ-ERDS-5.4.1-06 El ERDS generará y pondrá a disposición de las partes interesadas legítimas pruebas del ERDS sobre eventos de la ERD, tal como se definen en la cláusula 6 del ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 El prestador de servicio de entrega electrónica certificada (ERDSP) archivará las pruebas y/o los resúmenes de pruebas de cada prueba que haya expedido.

— REQ-ERDS-5.4.1-08 Las pruebas del ERDS generadas por él se ajustarán a la semántica de las pruebas que se establece en la cláusula 8 de ETSI EN 319 522-2 [4].

8) 7.2.1 Disposiciones comunes

— REQ-ERDS-7.2.1-02 El personal del ERDSP en funciones de confianza deberá ser capaz 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.

— REQ-ERDS-7.2.1-03 El cumplimiento de los requisitos de REQ-ERDS-7.2.1-02 incluirá actualizaciones periódicas (al menos cada doce meses) sobre las nuevas amenazas y las prácticas de seguridad actuales.

9) 7.3.2 Manipulación de soportes

— REQ-ERDS-7.3.1-02 Se aplicarán todos los requisitos de la norma ETSI EN 319 401 [1], apartado 7.3.3.

10) 7.5 Controles criptográficos

— REQ-ERDS-7.5-01A El ERDS seleccionará y utilizará técnicas criptográficas adecuadas conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [5].

— REQ-ERDSP-7.5-03 La clave privada de firma del ERDS 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 [6] 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

b) el esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) [7] [8] y con certificación EAL 4 o superior; o

c) hasta el 31.12.2030, FIPS PUB 140-3 [9] 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][8], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

11) 7.8 Seguridad de la red

— REQ-ERDSP-7.8-04 El ERDSP utilizará protocolos y algoritmos de vanguardia para el cifrado a nivel de la capa de transporte de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [5].

— REQ-ERDSP-7.8-06 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.

— REQ-ERDSP-7.8-07 La prueba de penetración exigida por REQ-7.8-17X de ETSI EN 319 401 [1] se realizará al menos una vez al año.

— REQ-ERDSP-7.8-08 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.

12) 7.12 Cese del ERDSP y planes de cese del ERDS

— REQ-ERDS-7.12-03 El plan de cese del ERDSP 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].

13) 7.14 Cadena de suministro

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

ANEXO II

Lista de normas y especificaciones de referencia a que se refiere el artículo 2

Se aplican las normas ETSI EN 319 522-1 V1.2.1 (2024-01) («ETSI EN 319 522-1»), ETSI EN 319 522-2 V1.2.1 (2024-01) («ETSI EN 319 522-2»), ETSI EN 319 522-3 V1.2.1 (2024-01) («ETSI EN 319 522-3») y ETSI EN 319 522-4-1 V1.2.1 (2019-01) («ETSI EN 319 522-4-1»), ETSI EN 319 522-4-2 V1.1.1 (2018-09) («ETSI EN 319 522-4-2») y ETSI EN 319 522-4-3 V1.1.1 (2018-09) («ETSI EN 319 522-4-3»).