2026/1735

22.7.2026

REGLAMENTO DE EJECUCIÓN (UE) 2026/1735 DE LA COMISIÓN

de 15 de julio de 2026

por el que se modifica el Reglamento de Ejecución (UE) 2025/1569 en lo que respecta a las normas y especificaciones aplicables

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 45 *quinquies*, apartado 5, su artículo 45 *sexies*, apartado 2, y su artículo 45 *septies*, apartados 6 y 7,

Considerando lo siguiente:

(1) A fin de garantizar el máximo nivel de armonización entre los Estados miembros para el desarrollo de las carteras europeas de identidad digital, las especificaciones técnicas de las carteras se basan en el trabajo realizado sobre la base de la Recomendación (UE) 2021/946 de la Comisión ([2]), y en particular en la arquitectura y el marco de referencia. Dado que la arquitectura y el marco de referencia han evolucionado significativamente desde la adopción del Reglamento de Ejecución (UE) 2025/1569 de la Comisión ([3]), dicho Reglamento de Ejecución debe modificarse ahora para adaptarlo a las nuevas normas, especificaciones y procedimientos.

(2) De conformidad con los objetivos del Reglamento (UE) n.º 910/2014, se han seleccionado una serie de normas para cumplir los requisitos aplicables a la expedición, gestión y verificación de las declaraciones electrónicas de atributos. Estas normas deben reflejar las prácticas establecidas y ser ampliamente aceptadas en los sectores pertinentes. Cuando sea necesario, estas normas deben adaptarse o complementarse para garantizar un elevado nivel de seguridad e integridad de las declaraciones electrónicas de atributos, facilitando al mismo tiempo la interoperabilidad transfronteriza y el funcionamiento eficaz del mercado interior. En consonancia con este objetivo, el presente Reglamento actualiza los requisitos aplicables a la expedición y revocación de declaraciones electrónicas cualificadas de atributos y declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica o en nombre de este e introduce los requisitos para la firma y el sellado de los resultados de la verificación frente a fuentes auténticas.

(3) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([4]) y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([5]) 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]) Recomendación (UE) 2021/946 de la Comisión, de 3 de junio de 2021, sobre un conjunto de instrumentos común de la Unión para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea (DO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Reglamento de Ejecución (UE) 2025/1569 de la Comisión, de 29 de julio 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 declaraciones electrónicas cualificadas de atributos y las declaraciones electrónicas de atributos proporcionadas por un organismo del sector público responsable de una fuente auténtica, o en nombre de este (DO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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).

(4) 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 ([6]) emitió su dictamen el 17 de abril de 2026 ([7]).

(5) 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

Modificaciones del Reglamento de Ejecución (UE) 2025/1569

El Reglamento de Ejecución (UE) 2025/1569 se modifica como sigue:

1) En el artículo 3, el apartado 2 se sustituye por el texto siguiente:

«2. Cuando los prestadores de declaraciones electrónicas de atributos cualificadas y los prestadores de declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica, o en nombre de este, expidan declaraciones electrónicas de atributos que estén incluidas en sistemas registrados en el catálogo de sistemas para la declaración de atributos, cumplirán los requisitos del sistema para la declaración de atributos correspondiente. Las políticas y los procedimientos establecidos por los emisores de declaraciones para cumplir los requisitos de los sistemas para la declaración de atributos formarán parte de la evaluación de la conformidad establecida en el Reglamento (UE) n.º 910/2014.».

2) El artículo 4 se modifica como sigue:

a) se suprime el apartado 1;

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

«3. Los prestadores de declaraciones electrónicas cualificadas de atributos y los prestadores de declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica, o en nombre de este, revocarán esas declaraciones, siempre que se hayan expedido con un período de validez de más de veinticuatro horas, al menos en las circunstancias siguientes:

a) cuando lo solicite la persona a la que se haya expedido la declaración electrónica de atributos o, cuando proceda, el sujeto de la declaración;

b) cuando el prestador tenga conocimiento de que se ha puesto en peligro la seguridad o la fiabilidad de las declaraciones electrónicas cualificadas de atributos o de las declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica, o en nombre de este;

c) en otras situaciones, cuando así lo exija el Derecho de la Unión o nacional.»;

c) el apartado 4 se sustituye por el texto siguiente:

«4. Los prestadores de declaraciones electrónicas cualificadas de atributos y los prestadores de declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica, o en nombre de este, establecerán técnicas de revocación y métodos de gestión que protejan la privacidad y dificulten la vinculación o la trazabilidad. Las técnicas de revocación cumplirán los requisitos establecidos en el anexo II.».

([6]) 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).

([7]) EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties | [«Observaciones formales del SEPD sobre el proyecto de Reglamento de Ejecución de la Comisión en lo que respecta a las normas y especificaciones aplicables al registro de partes usuarias de la cartera», documento en inglés]. Supervisor Europeo de Protección de Datos.

3) El artículo 9 se modifica como sigue:

a) tras el apartado 2 se añade el siguiente apartado 2 *bis*:

«2 *bis*. El mecanismo de verificación cumplirá las especificaciones establecidas en el anexo IV.»;

b) el apartado 4 se sustituye por el texto siguiente:

«4. El resultado de la verificación mencionará si el atributo ha sido verificado o no y especificará el organismo del sector público responsable de la fuente auténtica o, cuando proceda, el organismo del sector público designado para actuar en nombre de la fuente auténtica con la que se ha cotejado el atributo.

El resultado de la verificación será firmado o sellado por el organismo del sector público responsable de una fuente auténtica, o por el intermediario designado reconocido a nivel nacional, utilizando al menos una firma electrónica avanzada basada en un certificado cualificado de firma electrónica o un sello electrónico avanzado basado en un certificado cualificado de sello electrónico, respectivamente.».

4) El anexo I se sustituye por el texto que figura en el anexo I del presente Reglamento.

5) El anexo II se sustituye por el texto que figura en el anexo II del presente Reglamento.

6) El texto del anexo III del presente Reglamento se añade como anexo IV.

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 artículo 1, apartado 3, será aplicable a partir del 1 de enero de 2027.

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

Hecho en Bruselas, el 15 de julio de 2026.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

«*ANEXO I*

Lista de normas y especificaciones de referencia a que se refiere el artículo 3

Se aplicará la ETSI TS 119 471 V1.1.1 (2025-05), con las adaptaciones siguientes:

1) 2.1 Referencias normativas:

[1] ETSI EN 319 401 V3.2.1 (2026-01): Electronic Signatures and Trust Infrastructures (ESI) ["Firmas electrónicas e infraestructuras de confianza (ESI)"]; General Policy Requirements for Trust Service Providers ["Firmas electrónicas e infraestructuras de confianza (ESI). Requisitos de política general para prestadores de servicios de confianza", documento en inglés];

[2] 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] FIPS PUB 140-3 (2019) "Security Requirements for Cryptographic Modules" ["Requisitos de seguridad para módulos criptográficos"].

[4] Reglamento de Ejecución (UE) 2024/482 de la Comisión ([1]);

[5] Reglamento de Ejecución (UE) 2024/3144 de la Comisión ([2]);

[6] 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:

Se añade el término siguiente:

— 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) 4. Servicios de confianza de declaraciones electrónicas de atributos

— No se aplicará la cláusula 4.2.2.2 "Verification of attributes against authentic sources" ["Verificación de atributos frente a fuentes auténticas"].

— REQ-EAASP-4.2.2.3-02: El prestador de declaraciones electrónicas de atributos autenticará ante la instancia de cartera europea de identidad digital los mecanismos de autenticación mutua que utilicen un certificado de acceso válido.

— REQ-EAASP-4.2.2.3-03: El prestador de declaraciones electrónicas de atributos validará la unidad de cartera europea de identidad digital y *si se revoca la instancia de cartera europea de identidad digital*.

— No se aplicará la cláusula 4.3.2 "EUDIW Specific" ["Específico de la cartera europea de identidad digital"].

4) 6.1 Declaración de prácticas de los servicios de declaraciones electrónicas de atributos:

— REQ-EAASP-6.1-02: El prestador de declaraciones electrónicas de atributos documentará el mecanismo de revocación en la declaración de prácticas de servicios de declaraciones electrónicas de atributos.

5) 6.3 Política de seguridad de la información:

— REQ-EAASP-6.3-02: El prestador de declaraciones electrónicas de atributos establecerá procedimientos para notificar al organismo de supervisión cualquier modificación en la prestación del servicio de declaraciones electrónicas de atributos y la intención de cesar dichas actividades, de conformidad con los requisitos empresariales y las disposiciones legales y reglamentarias pertinentes, también de conformidad con los requisitos de los actos de ejecución adoptados en virtud del artículo 24, apartado 5, del Reglamento (UE) n.º 910/2014. El prestador de servicios de confianza notificará al organismo de supervisión competente, como mínimo:

— cualquier modificación un mes antes de llevarla a cabo,

— el cese previsto de la prestación de un servicio de confianza tres meses antes de que se produzca.

([1]) Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, 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) (DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Reglamento de Ejecución (UE) 2024/3144 de la Comisión, de 18 de diciembre de 2024, por el que se modifica el Reglamento de Ejecución (UE) 2024/482 en lo relativo a las normas internacionales aplicables y se corrige dicho Reglamento de Ejecución (DO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

6) 7.5 Controles criptográficos:

— REQ-EAASP-7.5.2-05: sin efecto.

— REQ-EAASP-7.5.2-06: sin efecto.

— REQ-EAASP-7.5.3-01A: Se establecerán controles de seguridad adecuados para la gestión de las claves criptográficas, los algoritmos criptográficos y los dispositivos criptográficos a lo largo de todo su ciclo de vida, siguiendo, cuando proceda, un enfoque de agilidad criptográfica.

— REQ-EAASP-7.5.3-01B: A efectos de la prestación de sus servicios de confianza, el prestador de declaraciones electrónicas de atributos 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 [2].

— REQ-EAASP-7.5.3-02: El prestador de declaraciones electrónicas de atributos velará por que el dispositivo criptográfico seguro que utilice para la firma o el sello digitales de la declaración electrónica de atributos sea un dispositivo cualificado de creación de firma o sello y por que todas las demás firmas o sellos digitales utilizados para prestar el correspondiente servicio de confianza de declaración electrónica de atributos, o parte del mismo, se creen mediante 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 los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, versión 3.1 (CC3.1) hasta el 31.8.2027, o 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, o tal como se establece en la norma ISO/IEC 15408 [6], y con certificación EAL 4 o superior, o

b) el esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) [4] [5] y con certificación EAL 4 o superior, o

c) FIPS-140-2level 3, que se utilizará hasta 31.8.2027 para los sistemas certificados existentes o FIPS PUB 140-3 [3] nivel 3 hasta 31.12.2030.

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 [4][5], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

— REQ-EAASP-7.5.5-01: sin efecto.

— REQ-EAASP-7.5.5-02: sin efecto.

— REQ-EAASP-7.5.5-04: sin efecto.

7) 7.9 Vulnerabilidades y gestión de incidentes:

— REQ-EAASP-7.9-02: Las actividades de seguimiento tendrán en cuenta la sensibilidad de cualquier información recogida o analizada.

8) 7.12 Planes de cese del prestador de declaraciones electrónicas de atributos y de sus servicios:

— REQ-EAASP-7.12-04: El plan de cese del prestador de declaraciones electrónicas de atributos 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].».

ANEXO II

«*ANEXO II*

Especificaciones técnicas a que se refieren los artículos 3 y 4

Los prestadores de declaraciones electrónicas cualificadas de atributos y los prestadores de declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica, o en nombre de este, expedirán sus declaraciones de conformidad con al menos una de las normas establecidas en el anexo II del Reglamento de Ejecución (UE) 2024/2979 de la Comisión ([1]) y aplicarán las técnicas de revocación pertinentes, también establecidas en el anexo II del Reglamento de Ejecución (UE) 2024/2979.».

([1]) Reglamento de Ejecución (UE) 2024/2979 de la Comisión, de 28 de noviembre de 2024, 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 la integridad y las funcionalidades básicas de las carteras europeas de identidad digital (DO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

ANEXO III

«ANEXO IV

Lista de normas y especificaciones técnicas a que se refiere el artículo 9

Los mecanismos de verificación a que se refiere el artículo 9 se ajustarán a uno de los elementos que se indican a continuación, o a ambos, con las adaptaciones siguientes:

a) las especificaciones técnicas establecidas en la cláusula 6.1.1 de ETSI TS 119 478 V1.1.1 (2026-01) — Firmas electrónicas e infraestructuras de confianza (ESI); Especificación de interfaces relacionadas con fuentes auténticas;

   — REQ-ASIP-6.1.1.2-04-01 [CONDITIONAL]: En caso de que el atributeVerificationResult sea http://uri.etsi.org/19478/VerificationResult/Match o http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, el atributeVerificationResult podrá contener un elemento atributeValue.

   — REQ-ASIP-6.1.1.2-04-02 [CONDITIONAL]: En caso de que el atributeVerificationResult devuelto sea http://uri.etsi.org/19478/VerificationResult/Match y el atributeVerificationResult contenga un elemento atributeValue, el elemento atributeValue contendrá el valor indicado en la solicitud.

   — REQ-ASIP-6.1.1.2-04-03 [CONDITIONAL]: En caso de que el atributeVerificationResult devuelto sea http://uri.etsi.org/19478/VerificationResult/MatchWithVariation y el atributeVerificationResult contenga un elemento atributeValue, el elemento atributeValue contendrá el valor del atributo tal y como se haya almacenado en la fuente auténtica.

   — REQ-ASIP-6.1.1.2-06-04-01 [CONDITIONAL]: En caso de que el fragmentVerificationResult sea http://uri.etsi.org/19478/VerificationResult/Match o http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, el atributeVerificationResult podrá contener un elemento fragmentValue.

   — REQ-ASIP-6.1.1.2-06-04-02 [CONDITIONAL]: En caso de que el fragmentVerificationResult devuelto sea http://uri.etsi.org/19478/VerificationResult/Match y el atributeVerificationResult contenga un elemento fragmentValue, el elemento fragmentValue contendrá el valor indicado en la solicitud.

   — REQ-ASIP-6.1.1.2-06-04-03 [CONDITIONAL]: En caso de que el fragmentVerificationResult devuelto sea http://uri.etsi.org/19478/VerificationResult/MatchWithVariation y el atributeVerificationResult contenga un elemento fragmentValue, el elemento fragmentValue contendrá el valor del fragmento del atributo tal y como se haya almacenado en la fuente auténtica.

b) las especificaciones técnicas establecidas en la cláusula 6.2.3 de ETSI TS 119 478 V1.1.1 (2026-01) — Firmas electrónicas e infraestructuras de confianza (ESI); Especificación de interfaces relacionadas con fuentes auténticas.

   — REQ-ASIP-6.2.3.2.1-08-04: El elemento AttributeVerificationResponse puede incluir exactamente un elemento subordinado (“child element”) de la opción TextValue, XMLValue o AttributeProperties.».