2026/798

8.4.2026

REGLAMENTO DE EJECUCIÓN (UE) 2026/798 DE LA COMISIÓN

de 7 de abril de 2026

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 y especificaciones para la incorporación a distancia de usuarios a las carteras europeas de identidad digital por medios de identificación electrónica conformes con el nivel de seguridad sustancial junto con procedimientos adicionales de incorporación a distancia cuando la combinación cumpla los requisitos del nivel de seguridad alto

LA COMISIÓN 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 5 *bis*, apartado 24,

Considerando lo siguiente:

(1) La incorporación de los usuarios a las carteras europeas de identidad digital (en lo sucesivo, «carteras») es un paso crucial en lo que respecta a la verificación de la identidad de los usuarios de la cartera, la vinculación de los datos de identificación de la persona de los usuarios con sus carteras y con el dispositivo del usuario en el que se instalen las unidades de cartera.

(2) A fin de fomentar un alto nivel de confianza y seguridad, así como un enfoque armonizado en todos los Estados miembros para la incorporación de los usuarios de una cartera con procedimientos de incorporación a distancia junto con los medios de identificación electrónica conformes con el nivel de seguridad sustancial, el presente acto de ejecución establece especificaciones y procedimientos para facilitar la incorporación de los usuarios a la cartera europea de identidad digital por medios de identificación electrónica conformes con el nivel de seguridad sustancial, junto con procedimientos adicionales de incorporación a distancia que, en conjunto, cumplan los requisitos del nivel de seguridad alto.

(3) Estas normas deben reflejar las prácticas establecidas y ser ampliamente aceptadas en los sectores pertinentes. Tales normas deben adaptarse para incluir requisitos que garanticen la seguridad y fiabilidad de la incorporación de los usuarios.

(4) El Reglamento de Ejecución (UE) 2015/1502 de la Comisión ([2]) establece que cuando los medios de identificación electrónica se expidan con el nivel de seguridad alto, y teniendo en cuenta los riesgos de que se produzca un cambio en los datos de identificación de la persona, no es necesario repetir los procesos de prueba (o acreditación) y verificación de la identidad. Por lo tanto, en tal caso, los Estados miembros deberían aprovechan los medios de identificación electrónica expedidos con el nivel de seguridad alto también para el proceso de incorporación a efectos del presente Reglamento.

(5) Cuando los Estados miembros incorporen usuarios en carteras utilizando un medio de identificación electrónica que no haya sido notificado a la Comisión, el nivel de seguridad de dicho medio debe ser confirmado por un organismo de evaluación de la conformidad definido en el artículo 2, apartado 13, del Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([3]) o por un organismo equivalente y debe demostrarse que los resultados de este procedimiento anterior de expedición de un medio de identificación electrónica siguen siendo válidos.

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

([2]) Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DO L 235 de 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([3]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

(6) Si bien en el anexo se establecen los requisitos que deben cumplirse para que se alcance un nivel específico de acreditación de la identidad, no se ha establecido la equivalencia con respecto al nivel de seguridad definido en el artículo 8 del Reglamento (UE) n.º 910/2014. Por consiguiente, debe considerarse que los requisitos establecidos en el anexo aplican los del Reglamento de Ejecución (UE) 2015/1502 y deben ser cumplidos por el proveedor de datos de identificación de la persona o por una entidad que preste servicios de acreditación de la identidad en nombre de dicho proveedor.

(7) La Comisión evalúa periódicamente las nuevas tecnologías, prácticas y especificaciones técnicas. De conformidad con el considerando 75 del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo ([4]), la Comisión debe revisar y actualizar el presente Reglamento de Ejecución para mantenerlo en consonancia con la evolución mundial, las nuevas tecnologías, normas o especificaciones técnicas y seguir las mejores prácticas del mercado interior, en particular en lo que respecta a la incorporación de usuarios a la cartera.

(8) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([5]) y, en aquellos casos en que proceda, el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([6]) y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([7]) son aplicables a todas las actividades de tratamiento de datos personales en virtud del presente Reglamento.

(9) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 emitió su dictamen el 30 de enero de 2026 ([8]).

(10) El comité establecido por el artículo 48 del Reglamento (UE) n.º 910/2014 no ha emitido dictamen alguno en el plazo establecido por su presidente.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Las normas y especificaciones de referencia a que se refiere el artículo 5 *bis*, apartado 24, del Reglamento (UE) n.º 910/2014 figuran en el anexo del presente Reglamento.

([4]) 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]) 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).

([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]) 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).

([8]) EDPS Formal comments on the draft Commission Implementing Regulation as regards onboarding of users to the European Digital Identity Wallets (Observaciones formales del Supervisor Europeo de Protección de Datos relativas al Reglamento de Ejecución de la Comisión en lo que respecta a la incorporación de usuarios a las carteras europeas de identidad digital, documento en inglés).

Artículo 2

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 7 de abril de 2026.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

LISTA DE NORMAS DE REFERENCIA Y ESPECIFICACIONES

La conformidad se evalúa con arreglo a las cláusulas de ETSI TS 119 461 V2.1.1 (2025-02) enumeradas en la sección 1, con sujeción a las adaptaciones enumeradas en la sección 2.

Sección 1 — Cláusulas aplicables

— 5 *Operational risk assessment;*

— 6 *Policies and practices*;

— 7 *Identity proofing service management and operation*;

— 8 *Identity proofing service requirements*;

— 9.1 *Introduction, compliance with the present document, general requirements for all use cases*;

— 9.2.2 *Use cases using an identity document for attended remote identity proofing*;

— 9.2.3 *Use cases using an identity document for unattended remote identity proofing*;

— 9.2.4 *Use case for identity proofing by authentication using eID means*;

— 9.5 *Use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Extended LoIP*.

Sección 2 — Adaptaciones

1) 5 Operational risk assessment

— OVR-5-01: Se aplicarán los requisitos especificados en la norma ETSI EN 319401 [1], cláusula 5.

— *Nota 1:* Cuando la acreditación de la identidad sea realizada por el propio proveedor de datos de identificación de la persona, la evaluación de riesgos del proveedor de datos de identificación de la persona puede abarcar la acreditación de la identidad.

2) 6.1 Identity proofing service practice statement

— OVR-6.1-02: Los prestadores de servicios de acreditación de la identidad (IPSP) identificarán en su declaración de prácticas los casos de uso para los que se declara la conformidad con el presente documento.

— *Nota 1:* Cuando la acreditación de la identidad sea realizada por el propio proveedor de datos de identificación de la persona, la declaración de prácticas del servicio de acreditación de la identidad del proveedor de datos de identificación de la persona puede abarcar la información sobre la acreditación de la identidad y no será necesaria ninguna declaración de prácticas específica para la acreditación de la identidad.

3) 7.9 Vulnerabilities and incident management

— OVR-7.9-02: Las obligaciones de notificación con arreglo a la norma ETSI EN 319401 [1], REQ-7.9.2-02X y cláusula 7.9.3, se cumplirán según lo exigido por el contexto de la acreditación de la identidad y las obligaciones del proveedor de datos de identificación de la persona que se base en el servicio del IPSP.

— EJEMPLO: La notificación a la autoridad de control que supervise a un proveedor de carteras europeas de identidad digital establecido en el Estado miembro que efectúa la designación puede llevarse a cabo en cooperación entre el IPSP y el proveedor de datos de identificación de la persona.

4) 7.10 Collection of evidence

— OVR-7.10-01: Se aplicarán los requisitos especificados en la norma ETSI EN 319401 [1], cláusula 7.10.

— *Nota 1:* Los requisitos a largo plazo para la conservación de pruebas pueden ser cumplidos por el proveedor de datos de identificación de la persona que solicita la acreditación de la identidad en lugar de por el IPSP cuando ambos sean entidades diferentes.

— *Nota 2:* Se aplican los requisitos del punto 8.5.2 del presente documento.

5) 7.11 Business continuity management

— OVR-7.11-02: Los procesos para la gestión de crisis con arreglo a la norma ETSI EN 319401 [1], REQ-7.11.3-01X, serán los requeridos por el contexto de la acreditación de la identidad y las obligaciones del proveedor de datos de identificación de la persona que se base en el servicio del IPSP.

6) 7.12 Termination and termination plans

— OVR-7.12-01: Se aplicarán los requisitos especificados en la norma ETSI EN 319401 [1], cláusula 7.12, excepto REQ-7.12-11.

— *Nota:* Cuando el IPSP y el proveedor de datos de identificación de la persona que solicita la acreditación de la identidad sean entidades diferentes, pueden acordar una asistencia mutua o unilateral a la hora de establecer planes de cese.

7) 8.1 Initiation

— INI-8.1-05: En caso de que el proceso de acreditación de la identidad a distancia se interrumpa o falle, el IPSP garantizará que se proporcionen a las personas explicaciones suficientes y vías de recurso, en particular en el caso de la acreditación de la identidad a distancia no atendida. La información debe garantizar que las personas puedan contribuir eficazmente a la rápida resolución del problema y, en caso necesario, ejercer sus derechos como interesados, como el derecho de rectificación o la posibilidad de impugnar la decisión, contra el responsable del tratamiento pertinente.

8) 8.2.1 General requirements

— COL-8.2.1-08: El IPSP aplicará medidas para garantizar el cumplimiento de los requisitos de protección de datos desde el diseño y por defecto de conformidad con el artículo 25 del Reglamento (UE) 2016/679 durante el proceso de incorporación, especialmente en lo que respecta al tratamiento de datos biométricos. Las medidas pertinentes podrán consistir en controles criptográficos, dispositivos y medidas organizativas adecuados que mejoren la privacidad. Tales medidas deben limitar la recogida de datos a lo estrictamente necesario para el tratamiento de los datos biométricos y cualquier otro dato personal que deba recogerse de las fuentes físicas y digitales de identificación a fin de vincular los datos de identificación personal del usuario a sus carteras y al dispositivo del usuario en el que esté instalada la unidad de cartera.

9) 8.2.4 Use of existing eID means as evidence

— [CONDICIONAL] COL-8.2.4-02X: Si el objetivo es el nivel básico de acreditación de la identidad (*Baseline LoIP*), los medios de identificación electrónica deberán haber sido notificados al menos como de un nivel de seguridad eIDAS sustancial o su nivel de seguridad deberá haber sido confirmado por un organismo de evaluación de la conformidad acreditado, tal como se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008, o por un organismo equivalente, y, si se cumplen todos los requisitos aplicables, la evaluación dará lugar a un certificado de conformidad basado en una auditoría de certificación. Este proceso de certificación formal se basará en un proceso de evaluación de la seguridad que se refiera a los niveles de seguridad definidos para los medios de identificación electrónica notificados o para las carteras europeas de identidad digital certificadas en virtud del Reglamento (UE) n.º 910/2014 [i.25].

— COL-8.2.4-02A: sin efecto.

10) 8.3.1 General requirements

— VAL-8.3.1-11X: El proceso de acreditación de la identidad verificará que las pruebas sean válidas en el momento de la acreditación de la identidad.

11) 8.3.3 Validation of physical identity document

— VAL-8.3.3-21: La eficacia de las medidas para cumplir los requisitos VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A y VAL-8.3.3-07X será confirmada por un organismo de evaluación de la conformidad acreditado, tal como se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008, o por un organismo equivalente.

— VAL-8.3.3-22: La imagen facial de referencia del documento físico de identidad se recogerá utilizando la comunicación de campo cercano y el proceso llevará a cabo la autenticación pasiva o activa del chip del documento físico de identidad.

12) 9.1 Introduction, compliance with the present document, general requirements for all use cases

— USE-9.1-01X: Para ser conformes con el presente documento, los procesos de acreditación de la identidad se ajustarán al caso de uso de la cláusula 9.5 del presente documento para el nivel ampliado de acreditación de la identidad (*Extended LoIP*).

— USE-9.1-03X: sin efecto.

13) 9.2.3.4 Use case for automated operation

— USE-9.2.3.4-04: El IPSP establecerá valores objetivo para la tasa de falsa aceptación (FAR) y la tasa de falso rechazo (RRF), sobre la base de un análisis de riesgos y su procedimiento de inteligencia sobre amenazas, siguiendo la metodología establecida en el informe de ENISA «Methodology for sectoral cybersecurity assessments» («Metodología para las evaluaciones sectoriales de la ciberseguridad», documento en inglés) [i.28] o una metodología equivalente, en procesos de acreditación de identidad totalmente automatizados. Los valores objetivo utilizados por el IPSP serán iguales o inferiores a los establecidos para los casos de uso de carácter híbrido, cuando existan. El IPSP mantendrá estos valores objetivo para la FAR y la RRF de manera coherente, con el apoyo de un análisis de riesgos y su procedimiento de inteligencia sobre amenazas.

14) 9.5.1 General requirements

— Primer apartado: Cuando el solicitante sea una persona física, también una persona física que represente a una persona jurídica, y se haya acreditado la identidad del solicitante al nivel básico de acreditación de la identidad (*Baseline LoIP*) mediante autenticación utilizando una identificación electrónica, y se requiera un refuerzo hasta el *Extended LoIP*, se aplicarán los requisitos siguientes.

— USE-9.5.1-08: La acreditación de la identidad adicional necesaria para reforzar la fiabilidad de una identidad solo es aplicable a la identificación electrónica que no se haya expedido basándose en una comparación automatizada entre imágenes faciales para el proceso de expedición inicial.

15) 9.5.2 Use case for enhancing identity proofing to Extended LoIP by a full identity proofing using an identity document

— USE-9.5.2-01: La acreditación de la identidad a fin de pasar del *Baseline LoIP* al *Extended LoIP* se ajustará a los requisitos del nivel ampliado de acreditación de la identidad de uno de los casos de uso descritos en las cláusulas 9.2.2 o 9.2.3 del presente documento para el *Extended LoIP*.

16) 9.5.3 Use case for enhancing identity proofing to Extended LoIP by use of a previously captured reference face image

— USE-9.5.3-01: Para captar una imagen facial de referencia y vincular los atributos de identidad necesarios a dicha imagen, se utilizará un proceso de acreditación de la identidad que cumpla los requisitos del *Extended LoIP* de uno de los casos de uso descritos en las cláusulas 9.2.2 o 9.2.3 del presente documento, o el proceso de acreditación de la identidad ha sido revisado por pares o certificado por un organismo de evaluación de la conformidad acreditado definido en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008 o un organismo equivalente para cumplir el nivel de seguridad alto con arreglo al Reglamento (UE) n.º 910/2014 [i.25].