



REGLAMENTO DE EJECUCIÓN (UE) 2025/848 DE LA COMISIÓN

de 6 de mayo 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 relativo al registro de las partes usuarias de las carteras

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 5 *ter*, apartado 11,

Considerando lo siguiente:

- (1) A efectos del registro de las partes usuarias que tengan previsto utilizar carteras europeas de identidad digital (en lo sucesivo, «carteras») para prestar servicios públicos o privados digitales, tal como lo exige el Reglamento (UE) n.º 910/2014, los Estados miembros deben establecer y mantener registros nacionales de las partes usuarias de las carteras establecidas en su territorio.
- (2) La Comisión evalúa periódicamente las nuevas tecnologías, prácticas, normas y especificaciones técnicas. Con el fin de garantizar el máximo nivel de armonización entre los Estados miembros para el desarrollo y la certificación de las carteras, las especificaciones técnicas establecidas en el presente Reglamento se basan en el trabajo realizado en virtud de la Recomendación (UE) 2021/946 de la Comisión⁽²⁾ y en particular la arquitectura y el marco de referencia que forman parte de él. De conformidad con el considerando 75 del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo⁽³⁾, la Comisión debe revisar y, en caso necesario, actualizar el presente Reglamento, para mantenerlo en consonancia con la evolución mundial, la arquitectura y el marco de referencia y seguir las mejores prácticas en el mercado interior.
- (3) Para garantizar un amplio acceso a los registros y lograr la interoperabilidad, los Estados miembros deben establecer interfaces legibles tanto por el ser humano como por máquina que cumplan las especificaciones técnicas establecidas en el presente Reglamento. Es preciso que los proveedores de certificados de acceso de parte usuaria de la cartera y de certificados de registro de parte usuaria de la cartera, cuando se disponga de ellos, puedan utilizar también estas interfaces para la expedición de dichos certificados.
- (4) Dado que las políticas de registro proporcionan a las partes usuarias de las carteras una orientación clara sobre el proceso de registro, los Estados miembros deben establecer y publicar las políticas de registro aplicables a los registros nacionales establecidos en su territorio.
- (5) La finalidad del registro de las partes usuarias de las carteras es generar confianza en el uso de las carteras gracias a una mayor transparencia. Por consiguiente, los Estados miembros deben poner a disposición del público la información pertinente de manera legible tanto por el ser humano como por máquina. A tal fin, las partes usuarias de las carteras deben facilitar la información necesaria, incluida la relativa a su habilitación o habilitaciones, a los registros nacionales.
- (6) Además, para mayor transparencia, las partes usuarias de las carteras deben declarar si tienen intención de recurrir a la identificación electrónica de personas físicas.
- (7) Para garantizar que el proceso de registro sea eficaz en relación con los costes y proporcionado al riesgo, los registradores deben establecer procesos de registro en línea y, cuando proceda, automatizados que sean fáciles de utilizar para las partes usuarias de las carteras. Es preciso que los registradores verifiquen las solicitudes de registro sin demora indebida.

⁽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 (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>).

- (8) Los Estados miembros deben garantizar que las carteras puedan autenticar a las partes usuarias de las carteras, con independencia del lugar de la Unión en el que estén establecidas. Para ello, las partes usuarias de las carteras deben utilizar certificados de acceso de parte usuaria de la cartera cuando se identifiquen en unidades de cartera. A fin de garantizar la interoperabilidad de esos certificados entre todas las carteras proporcionadas dentro de la Unión, los certificados de acceso de parte usuaria de la cartera deben ajustarse a unos requisitos comunes establecidos en el anexo. La Comisión debe elaborar políticas de certificación y declaraciones de prácticas de certificación armonizadas que deben aplicar los Estados miembros. La Comisión, en colaboración con los Estados miembros, debe supervisar de cerca la elaboración de normas nuevas o alternativas que puedan servir de base para implementar los certificados de acceso de las partes usuarias. En particular, deben evaluarse los modelos de confianza cuya eficacia y seguridad hayan quedado comprobadas en los Estados miembros.
- (9) Tal como se establece en el Reglamento (UE) n.º 910/2014, las partes usuarias de las carteras no deben solicitar a los usuarios que faciliten otros datos que no sean los indicados para el uso previsto de las carteras durante el proceso de registro. Es preciso que los usuarios de una cartera puedan verificar los datos de registro de las partes usuarias de la cartera. Para que los usuarios de una cartera puedan verificar que los atributos solicitados por la parte usuaria de la cartera entran en el ámbito de sus atributos registrados, los Estados miembros pueden exigir que se expidan certificados de registro de parte usuaria de la cartera a las partes usuarias registradas. A fin de garantizar la interoperabilidad de los certificados de registro de parte usuaria de la cartera, los Estados miembros deben garantizar que dichos certificados cumplan los requisitos y las normas establecidos en el anexo. En particular, las partes usuarias de las carteras deben declarar si tienen intención de recurrir a la identificación electrónica de personas físicas para cumplir alguno de los requisitos establecidos en el artículo 6, apartado 1, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo⁽⁴⁾ con fines de transparencia. Además, las partes usuarias no deben rechazar el uso de seudónimos, cuando el Derecho de la Unión o nacional no exija la identificación del usuario.
- (10) A fin de proteger a los usuarios contra la divulgación excesiva de información a las partes usuarias de las carteras y de advertirles en tales casos, los Estados miembros deben incluir en sus políticas de certificación medidas comunes de acceso que permitan a una solución de cartera informar al usuario de una cartera siempre que una parte usuaria de la cartera solicite más información que aquella para la que se ha registrado o para la que ha sido autorizada a acceder.
- (11) Para proteger a los usuarios de una cartera, es preciso que los registradores puedan suspender o cancelar sin previo aviso el registro de cualquier parte usuaria de una cartera cuando tengan motivos para creer que el registro contiene información inexacta, obsoleta o engañosa, que la parte usuaria de la cartera no cumple la política de registro, o que la parte usuaria de la cartera está infringiendo el Derecho de la Unión o nacional o la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital⁽⁵⁾ de algún otro modo que guarde relación con su función como parte usuaria de la cartera, por ejemplo, si no ha minimizado debidamente el conjunto de atributos a los que solicita acceso. Para preservar la estabilidad del ecosistema de la cartera europea de identidad digital (el «ecosistema de la cartera»), la decisión de suspender o cancelar un registro debe ser proporcional a la perturbación del servicio causada por la suspensión o la cancelación y a los costes e inconvenientes conexos para el prestador de servicios y el usuario. De conformidad con el artículo 46 bis, apartado 4, letra f), del Reglamento (UE) n.º 910/2014, los organismos de supervisión también deben estar facultados para suspender y cancelar el registro en caso necesario.
- (12) A efectos de la supervisión posterior, de las investigaciones llevadas a cabo por las autoridades policiales y judiciales y de la tramitación de litigios, los registradores deben conservar durante diez años registros de toda la información facilitada por las partes usuarias de las carteras establecidas en su registro nacional.
- (13) El Reglamento (UE) 2016/679 y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo⁽⁶⁾ son aplicables a las actividades de tratamiento de datos personales en virtud del presente Reglamento.

(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) DO C 23 de 23.1.2023, p. 1.

(6) 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>).

- (14) 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 ⁽⁷⁾, emitió su dictamen el 31 de enero de 2025.
- (15) 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

Objeto y ámbito de aplicación

El presente Reglamento establece normas para el registro de las partes usuarias de las carteras.

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

- 1) «parte usuaria de la cartera»: parte que tiene la intención de utilizar unidades de cartera para la prestación de servicios públicos o privados mediante interacción digital;
- 2) «unidad de cartera»: configuración única de una solución de cartera que incluye instancias de cartera, aplicaciones criptográficas seguras de cartera y dispositivos criptográficos seguros de cartera proporcionados por un proveedor de carteras a un usuario particular de una cartera;
- 3) «solución de cartera»: combinación de *software*, *hardware*, servicios, ajustes y configuraciones, que incluye instancias de cartera, una o más aplicaciones criptográficas seguras de cartera y uno o más dispositivos criptográficos seguros de cartera;
- 4) «instancia de cartera»: aplicación instalada y configurada en el dispositivo o el entorno de un usuario de una cartera, que forma parte de una unidad de cartera y que el usuario de la cartera utiliza para interactuar con la unidad de cartera;
- 5) «aplicación criptográfica segura de cartera»: aplicación que gestiona activos críticos al estar vinculada a las funciones criptográficas y no criptográficas proporcionadas por el dispositivo criptográfico seguro de cartera y utilizarlas;
- 6) «dispositivo criptográfico seguro de cartera»: dispositivo resistente a las manipulaciones fraudulentas que proporciona un entorno vinculado a la aplicación criptográfica segura de cartera y utilizado por esta para proteger activos críticos y proporcionar funciones criptográficas para la ejecución segura de operaciones críticas;
- 7) «activos críticos»: activos contenidos en una unidad de cartera o relacionados con ella, de tan extraordinaria importancia que, si su disponibilidad, confidencialidad o integridad se vieran comprometidas, el efecto sobre la capacidad para utilizar la unidad de cartera sería muy grave y debilitante;
- 8) «proveedor de cartera»: persona física o jurídica que proporciona soluciones de cartera;
- 9) «usuario de una cartera»: usuario que tiene el control sobre la unidad de cartera;
- 10) «registro nacional de partes usuarias de las carteras»: registro electrónico nacional utilizado por un Estado miembro para poner a disposición del público la información sobre las partes usuarias de las carteras que están registradas en dicho Estado miembro, tal como se establece en el artículo 5 *ter*, apartado 5, del Reglamento (UE) n.º 910/2014;
- 11) «proveedor de certificados de acceso de parte usuaria de la cartera»: persona física o jurídica a la que un Estado miembro ha encomendado expedir certificados de acceso de parte usuaria de la cartera a las partes usuarias de las carteras registradas en ese Estado miembro;

(7) 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>).

- 12) «certificado de acceso de parte usuaria de la cartera»: certificado para sellos o firmas electrónicos, expedido por un proveedor de certificados de acceso de parte usuaria de la cartera, que autentica y valida a la parte usuaria de la cartera;
- 13) «proveedor de datos de identificación de la persona»: persona física o jurídica responsable de la expedición y la revocación de los datos de identificación de la persona y de garantizar que los datos de identificación de la persona de un usuario estén vinculados criptográficamente a una unidad de cartera;
- 14) «registrador de partes usuarias de las carteras»: el organismo, designado por un Estado miembro, responsable de establecer y mantener la lista de las partes usuarias de las carteras registradas establecidas en su territorio;
- 15) «certificado de registro de parte usuaria de la cartera»: objeto de datos que describe el uso previsto de la parte usuaria e indica los atributos que la parte usuaria ha registrado con el propósito de solicitárselos a los usuarios;
- 16) «proveedor de certificados de registro de parte usuaria de la cartera»: persona física o jurídica a la que un Estado miembro ha encomendado expedir certificados de registro de parte usuaria de la cartera a las partes usuarias de las carteras registradas en ese Estado miembro.

Artículo 3

Registros nacionales

1. Los Estados miembros constituirán y mantendrán al menos un registro nacional de partes usuarias de las carteras con información relativa a las partes usuarias de las carteras registradas que estén establecidas en ese Estado miembro.
2. El registro incluirá al menos la información que figura en el anexo I.
3. Los Estados miembros designarán al menos a un registrador para que administre y gestione al menos un registro nacional de partes usuarias de las carteras.
4. Los Estados miembros publicarán en línea, tanto en un formato legible por el ser humano como en un formato adecuado para el tratamiento automatizado, la información que se indica en el anexo I sobre las partes usuarias de las carteras registradas.
5. La información a la que se refiere el apartado 2 estará disponible a través de una única interfaz de programación de aplicaciones («API») común y de un sitio web nacional. Estará firmada o sellada electrónicamente por el registrador o en su nombre, de conformidad con los requisitos comunes para una API única establecidos en la sección 1 del anexo II.
6. Los Estados miembros se asegurarán de que la API a la que se refiere el apartado 5 cumpla los requisitos comunes establecidos en la sección 2 del anexo II.
7. Los Estados miembros se asegurarán de que los registros cumplan las políticas de registro comunes pertinentes establecidas en el artículo 4.

Artículo 4

Políticas de registro

1. Los Estados miembros instaurarán y publicarán una o varias políticas nacionales de registro aplicables a los registros nacionales establecidos en su territorio.
2. Los Estados miembros podrán incluir o reutilizar políticas de registro sectoriales o nacionales existentes.
3. La política nacional de registro incluirá, como mínimo, información sobre:
 - a) los procedimientos de identificación y autenticación aplicables a las partes usuarias de las carteras durante el proceso de registro;
 - b) la documentación justificativa requerida, relativa a la identidad, el registro mercantil, la habilitación o las habilitaciones aplicables y otra información pertinente sobre la parte usuaria de la cartera;
 - c) las fuentes auténticas u otros registros electrónicos oficiales y en qué casos se puede recurrir a dichas fuentes o registros para obtener datos exactos;

- d) cualquier otra información o prueba necesaria como parte del proceso de registro;
 - e) cuando proceda, los medios automatizados disponibles para que las partes usuarias de las carteras puedan registrarse o para actualizar un registro existente;
 - f) el mecanismo de recurso de que disponen las partes usuarias de las carteras en virtud de la legislación y los procedimientos del Estado miembro en el que esté establecido el registro nacional;
 - g) las normas y los procedimientos para la verificación de la identidad de las partes usuarias de las carteras registradas y de cualquier otra información pertinente facilitada por dichas partes.
4. Los procedimientos y la documentación a que se refiere el apartado 3, letras (a) y (b), permitirán a las partes usuarias de las carteras indicar la habilitación o las habilitaciones específicas en virtud de las cuales están actuando, tal como se establece en el anexo I.
5. Cuando proceda, los requisitos establecidos en la política nacional de registro no impedirán un proceso de registro automatizado.

Artículo 5

Información que debe facilitarse a los registros nacionales

1. Las partes usuarias de las carteras facilitarán al menos la información indicada en el anexo I a los registros nacionales.
2. Las partes usuarias de las carteras se asegurarán de que la información facilitada sea exacta en el momento del registro.
3. Las partes usuarias de las carteras actualizarán sin demora indebida cualquier información previamente inscrita en el registro nacional de partes usuarias de las carteras.

Artículo 6

Proceso de registro

1. Los registradores establecerán procesos de registro electrónicos y, cuando sea posible, automatizados fáciles de utilizar para las partes usuarias de las carteras.
2. Los registradores tramitarán las solicitudes de registro sin demora indebida y darán respuesta a la solicitud de registro del solicitante en el plazo definido en la política de registro aplicable, utilizando los medios adecuados y de conformidad con la legislación y los procedimientos del Estado miembro en el que esté establecido el registro nacional.
3. Siempre que sea posible, los registradores verificarán de manera automatizada:
 - a) la exactitud, la validez, la autenticidad y la integridad de la información exigida en virtud del artículo 5;
 - b) cuando proceda, el poder de representación de los representantes de las partes usuarias de las carteras redactado y presentado de conformidad con la legislación y los procedimientos del Estado miembro en el que esté establecido el registro nacional;
 - c) el tipo de habilitación o habilitaciones de las partes usuarias de las carteras, tal como se establece en el anexo I;
 - d) la ausencia de inscripción en otro registro nacional.
4. Los registradores cotejarán la información indicada en el apartado 3 con la documentación justificativa proporcionada por las partes usuarias de las carteras o con las fuentes auténticas adecuadas u otros registros electrónicos oficiales del Estado miembro en el que esté establecido el registro nacional y a los que tengan acceso los registradores de conformidad con la legislación y los procedimientos nacionales aplicables.
5. La verificación de las habilitaciones de las partes usuarias de las carteras a que se refiere el apartado 3, letra (c) se llevará a cabo de conformidad con el anexo III.
6. Cuando el registrador no pueda verificar la información de conformidad con lo dispuesto en los apartados 3 a 5, rechazará el registro.

7. Cuando una parte usuaria de cartera ya no tenga la intención de confiar en unidades de cartera para la prestación de servicios públicos o privados en el marco de un registro específico, lo notificará sin demora indebida al registrador pertinente y solicitará la cancelación de ese registro.

Artículo 7

Certificados de acceso de parte usuaria de la cartera

1. Los Estados miembros autorizarán al menos a una autoridad de certificación para que expida certificados de acceso de parte usuaria de la cartera.
2. Los Estados miembros se asegurarán de que los proveedores de certificados de acceso de parte usuaria de la cartera expidan estos certificados de acceso exclusivamente a las partes usuarias de las carteras registradas.
3. Los Estados miembros aplicarán de manera sintáctica y semánticamente armonizada las políticas de certificación y las declaraciones de prácticas de certificación para los certificados de acceso de parte usuaria de la cartera, de conformidad con los requisitos establecidos en el anexo IV.

Artículo 8

Certificados de registro de parte usuaria de la cartera

1. Los Estados miembros podrán autorizar al menos a una autoridad de certificación para que expida certificados de registro de parte usuaria de la cartera.
2. Cuando un Estado miembro haya autorizado la expedición de un certificado de registro de una parte usuaria de la cartera, dicho Estado miembro:
 - a) exigirá a los proveedores de certificados de registro de parte usuaria de la cartera que expidan estos certificados de registro exclusivamente a las partes usuarias de las carteras registradas;
 - b) se asegurará que cada uso previsto esté explicitado en los certificados de registro de parte usuaria de la cartera;
 - c) se asegurará de que los certificados de registro de parte usuaria de la cartera incluyan una política general de acceso, armonizada sintáctica y semánticamente en toda la Unión, que informe a los usuarios de que la parte usuaria de la cartera solo está autorizada a solicitar los datos especificados en los certificados de registro para el uso previsto registrado en ellos;
 - d) se asegurará de que los proveedores de soluciones de cartera establecidos en ese Estado miembro cumplan la política general de acceso informando a los usuarios cuando una parte usuaria de cartera solicite datos que no estén especificados en los certificados de registro;
 - e) implementará los certificados de registro de parte usuaria de la cartera de manera armonizada sintáctica y semánticamente y en consonancia con los requisitos establecidos en el anexo V;
 - f) aplicará políticas de certificación y declaraciones de prácticas de certificación específicas para los certificados de registro de parte usuaria de la cartera, de conformidad con los requisitos establecidos en el anexo V;
 - g) se asegurará de que las partes usuarias de las carteras proporcionen una URL a la política de privacidad en relación con el uso previsto.
3. La política a la que se refiere la letra (g) se reflejará en el certificado de registro de la parte usuaria de la cartera.

Artículo 9

Suspensión y cancelación del registro

1. Los registradores suspenderán o cancelarán el registro de una parte usuaria de cartera cuando un organismo de supervisión solicite dicha suspensión o cancelación de conformidad con el artículo 46 bis, apartado 4, letra f), del Reglamento (UE) n.º 910/2014.
2. Los registradores podrán suspender o cancelar el registro de una parte usuaria de cartera cuando tengan motivos para creer que se da alguna de las siguientes circunstancias:
 - a) el registro contiene información inexacta, obsoleta o engañosa;

- b) la parte usuaria de la cartera no cumple la política de registro;
 - c) la parte usuaria de la cartera solicita más atributos de los que ha registrado de conformidad con el artículo 5 y el artículo 6;
 - d) la parte usuaria de la cartera está infringiendo el Derecho de la Unión o nacional de algún otro modo que guarde relación con su función como parte usuaria de la cartera.
3. Los registradores suspenderán o cancelarán el registro de una parte usuaria de la cartera cuando la propia parte usuaria de la cartera solicite la cancelación o la suspensión.
4. Al considerar la suspensión o la cancelación de conformidad con el apartado 2, el registrador llevará a cabo una evaluación de la proporcionalidad, teniendo en cuenta la repercusión en los derechos fundamentales, la seguridad y la confidencialidad de los usuarios en el ecosistema, así como la gravedad de la perturbación que se prevé que cause la suspensión o la cancelación y los costes asociados, tanto para la parte usuaria de la cartera como para el usuario. Sobre la base del resultado de esta evaluación, el registrador podrá suspender o cancelar el registro con o sin previo aviso a la parte usuaria de la cartera afectada.
5. Cuando el registro de una parte usuaria de la cartera se suspenda o se cancele, el registrador informará de ello, sin demora indebida y a más tardar veinticuatro horas después de la suspensión o la cancelación, al proveedor de los certificados de acceso de parte usuaria de la cartera pertinentes, al proveedor de los certificados de registro de parte usuaria de la cartera pertinentes y a la parte usuaria de la cartera afectada. Esta notificación incluirá información sobre los motivos de la suspensión o cancelación y sobre las vías de recurso disponibles.
6. El proveedor de certificados de acceso de parte usuaria de la cartera y el proveedor de certificados de registro de parte usuaria de la cartera revocarán sin demora indebida, cuando proceda, los certificados de acceso de parte usuaria de la cartera y los certificados de registro de parte usuaria de la cartera, respectivamente, de la parte usuaria de la cartera cuyo registro se haya suspendido o cancelado.

Artículo 10

Conservación de los registros

Los registradores conservarán durante diez años los registros de la información facilitada por las partes usuarias de las carteras y registrada de conformidad con el anexo I para el registro de una parte usuaria de la cartera y la expedición de los certificados de acceso de parte usuaria de la cartera y los certificados de registro de parte usuaria de la cartera, así como de cualquier modificación posterior de esta información.

Artículo 11

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Será aplicable a partir del 24 de diciembre de 2026.

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

Hecho en Bruselas, el 6 de mayo de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

Información relativa a las partes usuarias de las carteras

1. Cuando proceda, el nombre de la parte usuaria de la cartera, como figure en un registro oficial, junto con los datos de identificación de dicho registro oficial.
 - a) si no es aplicable, se seguirá lo dispuesto en el apartado 2.
2. Cuando proceda, un nombre fácil de usar de la parte usuaria de la cartera, que puede ser un nombre comercial o un nombre de servicio reconocible para el usuario.
3. Cuando proceda, uno o varios identificadores de la parte usuaria de la cartera, tal y como figuren en un registro oficial, junto con los datos de identificación de dicho registro oficial, expresados como:
 - a) un número de registro e identificación de agente económico (EORI) como el mencionado en el Reglamento de Ejecución (UE) n.º 1352/2013 de la Comisión ⁽¹⁾;
 - b) un número de registro tal y como esté inscrito en un registro mercantil nacional;
 - c) un identificador de entidad jurídica (LEI) como el mencionado en el Reglamento de Ejecución (UE) n.º 2022/1860 de la Comisión ⁽²⁾;
 - d) un número de identificación a efectos del impuesto sobre el valor añadido («IVA»);
 - e) un número de impuestos especiales como el mencionado en el artículo 2, punto 12, del Reglamento (UE) n.º 389/2012 del Consejo ⁽³⁾;
 - f) un número de identificación fiscal;
 - g) un identificador único europeo (EUID) como el mencionado en el Reglamento de Ejecución (UE) n.º 2021/1042 de la Comisión ⁽⁴⁾;
 - h) otro identificador nacional u otros identificadores nacionales.
4. La dirección física en la que está establecida la parte usuaria de la cartera.
5. Cuando proceda, un localizador uniforme de recursos («URL») perteneciente a la parte usuaria de la cartera.
6. Cuando el identificador se exprese de conformidad con el punto 3, letras (a), (d), (f) o (h), el indicador de país del Estado miembro en el que la parte usuaria de la cartera esté establecida estará fijado previamente utilizando los códigos de país alfa-2 especificados en la norma ISO 3166-1, con excepción del indicador de país para Grecia, que será «EL».
7. Información de contacto de la parte usuaria de la cartera, indicando al menos uno de los siguientes datos:
 - a) un sitio web en el que se pueda contactar con la parte usuaria de la cartera para cuestiones relativas a la prestación de asistencia y apoyo;
 - b) un número de teléfono en el que se pueda contactar con la parte usuaria de la cartera para cuestiones relacionadas con su registro y el uso previsto de las unidades de cartera;
 - c) una dirección de correo electrónico en la que se pueda contactar con la parte usuaria de cartera para cuestiones relacionadas con su registro y el uso previsto de la unidad de cartera.
8. Una descripción del tipo de servicios prestados por la parte usuaria de la cartera.

⁽¹⁾ Reglamento de Ejecución (UE) n.º 1352/2013 de la Comisión, de 4 de diciembre de 2013, por el que se establecen los formularios previstos en el Reglamento (UE) n.º 608/2013 del Parlamento Europeo y del Consejo, relativo a la vigilancia por parte de las autoridades aduaneras del respeto de los derechos de propiedad intelectual (DO L 341 de 18.12.2013, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

⁽²⁾ Reglamento de Ejecución (UE) 2022/1860 de la Comisión, de 10 de junio de 2022, por el que se establecen normas técnicas de ejecución para la aplicación del Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo por lo que respecta a los estándares, los formatos, la frecuencia y los métodos y mecanismos de notificación (DO L 262 de 7.10.2022, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

⁽³⁾ Reglamento (UE) n.º 389/2012 del Consejo, de 2 de mayo de 2012, sobre cooperación administrativa en el ámbito de los impuestos especiales y por el que se deroga el Reglamento (CE) n.º 2073/2004 (DO L 121 de 8.5.2012, p. 1, ELI: <http://data.europa.eu/eli/reg/2012/389/oj>).

⁽⁴⁾ Reglamento de Ejecución (UE) 2021/1042 de la Comisión, de 18 de junio de 2021, por el que se establecen disposiciones de aplicación de la Directiva (UE) 2017/1132 del Parlamento Europeo y del Consejo en lo que respecta a las especificaciones y los procedimientos técnicos necesarios para el sistema de interconexión de registros, y por el que se deroga el Reglamento de Ejecución (UE) 2020/2244 de la Comisión (DO L 225 de 25.6.2021, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2021/1042/oj).

9. Para cada uso previsto, una lista de los datos, incluidas las declaraciones y los atributos, que la parte usuaria tiene intención de solicitar, un nombre fácil de usar y un nombre técnico, el tipo de declaración y cualquier otra sintaxis en la que se agrupen los datos, en un formato legible por máquina para el tratamiento automatizado.
10. Para cada uso previsto, una descripción del uso previsto de los datos que la parte usuaria de la cartera tiene intención de solicitar a las unidades de cartera.
11. Una indicación de si la parte usuaria de la cartera es un organismo del sector público.
12. La habilitación o las habilitaciones de la parte usuaria de la cartera, expresadas de la siguiente manera:
 - a) «Service_Provider» para expresar la habilitación de la parte usuaria de la cartera como prestador de servicios;
 - b) «QEAA_Provider» para expresar la habilitación de la parte usuaria de la cartera como prestador cualificado de servicios de confianza que expide declaraciones electrónicas cualificadas de atributos;
 - c) «Non_Q_EAA_Provider» para expresar la habilitación de la parte usuaria de la cartera como prestador de servicios de confianza que expide declaraciones electrónicas no cualificadas de atributos;
 - d) «PUB_EAA_Provider» para expresar la habilitación de la parte usuaria de la cartera como proveedora de declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica o en nombre de este;
 - e) «PID_Provider» para expresar la habilitación de la parte usuaria de la cartera como proveedor de datos de identificación de la persona;
 - f) «QCert_for_ESeal_Provider» para expresar la habilitación de la parte usuaria de la cartera como prestador cualificado de servicios de confianza que expide certificados cualificados para sellos electrónicos;
 - g) «QCert_for_ESig_Provider» para expresar la habilitación de la parte usuaria de la cartera como prestador cualificado de servicios de confianza que expide certificados cualificados para firmas electrónicas;
 - h) «rQSigCDson Provider» para expresar la habilitación de la parte usuaria de la cartera como prestador cualificado de servicios de confianza que presta un servicio de confianza cualificado para la gestión de un dispositivo cualificado de creación de firma electrónica a distancia;
 - i) «rQSealCDS Provider» para expresar la habilitación de la parte usuaria de la cartera como prestador cualificado de servicios de confianza que presta servicios de confianza cualificados para la gestión de un dispositivo cualificado de creación de sello electrónico a distancia;
 - j) «ESig_ESeal_Creation_Provider» para expresar la habilitación de la parte usuaria de la cartera como prestador no cualificado de servicios de confianza que presta un servicio de confianza no cualificado para la creación de firmas electrónicas o sellos electrónicos a distancia.
13. Por lo que respecta al punto 12, letra (c), los Estados miembros podrán conceder otras subcategorías de habilitaciones para exponer qué declaraciones expedirá determinado emisor no cualificado de declaraciones electrónicas de atributos.
14. Cuando proceda, una indicación de que la parte usuaria de la cartera confía en un intermediario que actúa en nombre de la parte usuaria que tiene intención de utilizar la cartera.
15. Cuando proceda, un enlace de asociación con el intermediario en el que confía la parte usuaria de la cartera que actúa en nombre de la parte usuaria que tiene intención de utilizar la cartera.

ANEXO II

1. REQUISITOS PARA LAS FIRMAS ELECTRÓNICAS O LOS SELLOS ELECTRÓNICOS APLICADOS A LA INFORMACIÓN FACILITADA SOBRE LAS PARTES USUARIAS DE LAS CARTERAS REGISTRADAS A QUE SE REFIERE EL ARTÍCULO 3
 - JavaScript Object Notation («JSON»);
 - 7515 IETF para firmas web JSON.
2. REQUISITOS RELATIVOS A LA API COMÚN ÚNICA A QUE SE REFIERE EL ARTÍCULO 3
 - 1) La API común única:
 - a) será una API REST que proporcione soporte a JSON como formato y firmada de conformidad con los requisitos pertinentes especificados en la sección 1;
 - b) permitirá que cualquier solicitante, sin autenticación previa, realice búsquedas en el registro y solicitudes de listas completas al registro, para obtener información sobre las partes usuarias de las carteras registradas, permitiendo correspondencias parciales basadas en parámetros definidos, que incluirán, cuando proceda, el número de registro mercantil u oficial de la parte usuaria de la cartera, el nombre de la parte usuaria de la cartera o la información a que se refieren el artículo 8, apartado 2, letra g), y el anexo I, puntos 12, 13, 14 y 15;
 - c) garantizará que las respuestas a las solicitudes a que se refiere la letra (b) que correspondan al menos a una parte usuaria de la cartera incluyan una o más menciones de información sobre las partes usuarias de las carteras registradas e información con arreglo al anexo I, los certificados de acceso de parte usuaria de la cartera y los certificados de registro de parte usuaria de la cartera actuales e históricos, pero excluyan la información de contacto que se indica en el anexo I, punto 4;
 - d) se publicará como OpenAPI versión 3, junto con la documentación y las especificaciones técnicas adecuadas que garanticen la interoperabilidad en toda la Unión;
 - e) proporcionará funciones de seguridad, incluida la seguridad por defecto y desde el diseño, para garantizar la disponibilidad e integridad de la API y la disponibilidad de información a través de ella.
 - 2) Las menciones a que se refiere la letra (c) se expresarán en forma de archivos JSON firmados o sellados electrónicamente, cuyo formato y estructura se ajusten a los requisitos sobre firmas o sellos electrónicos establecidos en la sección 1.

ANEXO III

Fuente de pruebas documentales para la verificación de las habilitaciones de las partes usuarias de las carteras a que se refiere el artículo 6

1. La verificación de que una parte usuaria de la cartera es un proveedor de declaraciones electrónicas cualificadas de atributos, un proveedor de certificados cualificados para firmas electrónicas o sellos electrónicos, o un prestador de un servicio de confianza cualificado para la gestión de dispositivos cualificados de creación de firma o sello electrónicos a distancia se basará en las listas de confianza nacionales publicadas de conformidad con el artículo 22 del Reglamento (UE) n.º 910/2014.
2. La verificación de que una parte usuaria de la cartera es un proveedor de declaraciones electrónicas no cualificadas de atributos o un proveedor de creación a distancia de firmas electrónicas o sellos electrónicos como servicio de confianza no cualificado se basará, cuando proceda, en las listas de confianza nacionales publicadas de conformidad con el artículo 22 del Reglamento (UE) n.º 910/2014, o, en el caso de los prestadores de servicios de confianza no cualificados que no estén registrados en las listas de confianza nacionales, en los procedimientos de verificación que los Estados miembros hayan establecido en sus políticas de registro conforme a lo dispuesto en el artículo 4.
3. La verificación de que una parte usuaria de la cartera es un proveedor de datos de identificación de la persona se basará en la lista de proveedores de datos de identificación de la persona publicada por la Comisión de conformidad con el artículo 5 bis, apartado 18, del Reglamento (UE) n.º 910/2014.
4. La verificación de que una parte usuaria de la cartera es un proveedor de declaraciones electrónicas de atributos expedidas por un organismo del sector público responsable de una fuente auténtica o en nombre de este se basará en la lista publicada por la Comisión de conformidad con el artículo 45 septies, apartado 3, del Reglamento (UE) n.º 910/2014.

ANEXO IV

Requisitos aplicables a los certificados de acceso de parte usuaria de la cartera a que se refiere el artículo 7

1. La política de certificación del acceso de parte usuaria de la cartera aplicable al suministro de certificados de acceso de parte usuaria de la cartera describirá los requisitos de seguridad aplicables a un certificado de acceso de parte usuaria de la cartera y las normas de aplicabilidad de dicho certificado, de modo que se puedan expedir estos certificados a las partes usuarias de las carteras y estas puedan utilizarlos en sus interacciones con soluciones de cartera.
2. La declaración de prácticas de certificación del acceso de parte usuaria de la cartera aplicable al suministro de certificados de acceso de parte usuaria de la cartera describirá las prácticas que emplea un proveedor de certificados de acceso de parte usuaria de la cartera para la expedición, la gestión, la revocación y el cambio de claves de los certificados de acceso de parte usuaria de la cartera.
3. La política de certificación y la declaración de prácticas de certificación aplicables al suministro de certificados de acceso de parte usuaria de la cartera estarán sintácticamente y semánticamente armonizadas en toda la Unión y, cuando proceda, cumplirán al menos los requisitos de la política de certificación normalizada («NCP») especificados en la norma ETSI EN 319411-1, versión 1.4.1 (2023-10), e incluirán:
 - a) una descripción clara de la jerarquía de infraestructura de clave pública y los itinerarios de certificación, desde los certificados de acceso de parte usuaria de la cartera de la entidad final hasta la parte superior de la jerarquía utilizada para expedirlos, indicando el ancla o las anclas de confianza previstas en dicha jerarquía y los itinerarios que deben basarse en el marco de confianza establecido de conformidad con el artículo 5 bis, apartado 18, del Reglamento (UE) n.º 910/2014;
 - b) una descripción exhaustiva de los procedimientos para la expedición de certificados de acceso de parte usuaria de la cartera, y en concreto para la verificación de la identidad y cualquier otro atributo de la parte usuaria de la cartera a la que se vaya a expedir un certificado de parte usuaria de la cartera;
 - c) la obligación de que los proveedores de certificados de acceso de parte usuaria de la cartera, cuando expidan un certificado de acceso de parte usuaria de la cartera, verifiquen que:
 - la parte usuaria de la cartera está incluida, con un estado de registro válido, en un registro nacional de partes usuarias de las carteras del Estado miembro en el que está establecida dicha parte;
 - toda información contenida en el certificado de acceso de parte usuaria de la cartera es exacta y coherente con la información de inscripción en el registro disponible en dicho registro;
 - d) una descripción exhaustiva de los procedimientos para la revocación de los certificados de acceso de parte usuaria de la cartera;
 - e) la obligación de que los proveedores de certificados de acceso de parte usuaria de la cartera apliquen medidas y procesos para:
 - hacer un seguimiento continuo de cualquier cambio en el registro nacional de partes usuarias de la cartera en el que estén registradas las partes usuarias de la cartera a las que hayan expedido certificados de acceso de parte usuaria de la cartera;
 - revocar, cuando los cambios así lo requieran, cualquier certificado de parte usuaria de la cartera que el proveedor haya expedido a la parte usuaria correspondiente, en particular cuando el contenido del certificado ya no sea exacto ni coherente con la información registrada, o cuando se suspenda o cancele el registro de dicha parte;
 - f) una descripción exhaustiva de los procedimientos y los mecanismos para la validación armonizada de los certificados de acceso de parte usuaria de la cartera en toda la Unión;
 - g) la obligación de que los proveedores de certificados de acceso de parte usuaria de la cartera permitan a las partes interesadas pertinentes, en concreto a las partes usuarias de la cartera en lo que respecta a sus propios certificados, a los organismos de supervisión y a las autoridades de protección de datos competentes, solicitar la revocación de los certificados de acceso de parte usuaria de la cartera;
 - h) la obligación de que los proveedores de certificados de acceso de parte usuaria de la cartera registren todas esas revocaciones en su base de datos de certificados y publiquen el estado de revocación del certificado a su debido tiempo, y en cualquier caso en un plazo de veinticuatro horas a partir de la recepción de la solicitud de revocación;

- i) la obligación de que los proveedores de certificados de acceso de parte usuaria de la cartera faciliten información sobre el estado de validez o revocación de los certificados de parte usuaria de la cartera que hayan expedido;
 - j) una descripción, cuando proceda, del modo en que un proveedor de certificados de acceso de parte usuaria de la cartera archiva todos los certificados de acceso de parte usuaria de la cartera que ha expedido, de conformidad con el estándar de solicitud de comentarios («RFC») 9162 de transparencia de la certificación, versión 2.0, del Grupo de Trabajo de Ingeniería de Internet («IETF»);
 - k) la obligación de que los certificados de acceso de parte usuaria de la cartera incluyan:
 - la ubicación en la que está disponible el certificado que da soporte a la firma electrónica avanzada o el sello electrónico avanzado en dicho certificado, para todo el itinerario de certificación que debe construirse hasta el ancla de confianza prevista en la jerarquía de infraestructura de clave pública utilizada por el proveedor;
 - una referencia procesable por máquina a la política de certificación y la declaración de prácticas de certificación aplicables;
 - la información a que se refiere el anexo I, puntos 1, 2, 3, 5, 6 y punto 7, letras (a), (b) y (c).
4. La revocación mencionada en el punto 3, letra (g), será efectiva inmediatamente después de su publicación.
 5. La información mencionada en el punto 3, letra (h), deberá proporcionarse al menos por cada certificado en cualquier momento, y al menos con posterioridad al período de validez del certificado, en un formato automatizado que sea fiable, gratuito y efectivo de conformidad con la política de certificación.
-

ANEXO V

Requisitos aplicables a los certificados de registro de parte usuaria de la cartera a que se refiere el artículo 8

1. La política de certificación del registro de parte usuaria de la cartera aplicable al suministro de certificados de registro de parte usuaria de la cartera describirá los requisitos de seguridad aplicables a un certificado de registro de parte usuaria de la cartera y las normas de aplicabilidad de dicho certificado, para su expedición a las partes usuarias de la cartera y su uso por estas en sus interacciones con soluciones de cartera. La política de certificación del registro de parte usuaria de la cartera se publicará en un formato legible por el ser humano.
2. La declaración de prácticas de certificación del registro de parte usuaria de la cartera aplicable al suministro de certificados de registro de parte usuaria de la cartera describirá las prácticas que emplea un proveedor de certificados de registro de parte usuaria de la cartera para la expedición, la gestión, la revocación y el cambio de claves de los certificados de registro de parte usuaria de la cartera y, cuando proceda, cómo se relacionan con los certificados de acceso de parte usuaria de la cartera expedidos a partes usuarias de la cartera. La declaración de prácticas de certificación del registro de parte usuaria de la cartera se publicará en un formato legible por el ser humano.
3. La política de certificación y la declaración de prácticas de certificación del registro de parte usuaria de la cartera aplicables al suministro de certificados de registro de parte usuaria de la cartera estarán sintácticamente y semánticamente armonizadas en toda la Unión y cumplirán al menos los requisitos de la política de certificación normalizada («NCP») aplicables especificados en la norma ETSI EN 319411-1, versión 1.4.1 (2023-10), e incluirán:
 - a) una descripción clara de la jerarquía de infraestructura de clave pública y los itinerarios de certificación, desde los certificados de registro de parte usuaria de la cartera de la entidad final hasta la parte superior de la jerarquía utilizada para expedirlos, indicando al mismo tiempo el ancla o las anclas de confianza previstas en dicha jerarquía y dichos itinerarios;
 - b) una descripción exhaustiva de los procedimientos para la expedición de certificados de registro de parte usuaria de la cartera, y en concreto para la verificación de la identidad y de cualquier atributo de la parte usuaria de la cartera a la que se vaya a expedir un certificado de parte usuaria de la cartera;
 - c) la obligación de que el proveedor de certificados de registro de parte usuaria de la cartera, cuando expida un certificado de registro de parte usuaria de la cartera, verifique que:
 - la parte usuaria de la cartera está incluida, con un estado de registro válido, en un registro nacional para partes usuarias de las carteras del Estado miembro en el que está establecida dicha parte;
 - la información contenida en el certificado de registro de parte usuaria de la cartera es exacta y coherente con la información de inscripción en el registro disponible en dicho registro;
 - el certificado de acceso de parte usuaria de la cartera es válido;
 - la descripción de los procedimientos para la revocación de los certificados de registro de parte usuaria de la cartera es exhaustiva;
 - d) la obligación de que el proveedor de certificados de registro de parte usuaria de la cartera aplique medidas y procesos relativos a:
 - el seguimiento automatizado continuo de cualquier cambio en el registro nacional de partes usuarias de la cartera en el que estén registradas las partes usuarias de la cartera a las que haya expedido certificados de registro de parte usuaria de la cartera;
 - la reexpedición del certificado de registro de parte usuaria de la cartera;
 - la revocación de cualquier certificado de registro de parte usuaria de la cartera que haya expedido a la parte usuaria de la cartera correspondiente, cuando esos cambios así lo exijan, en particular cuando el contenido del certificado ya no sea exacto ni coherente con la información registrada, o cuando se modifique, suspenda o cancele el registro de dicha parte usuaria;
 - e) una descripción exhaustiva de los procedimientos y los mecanismos para la validación armonizada de los certificados de registro de parte usuaria de la cartera;

- f) la obligación de que el proveedor de certificados de registro de parte usuaria de la cartera permita a las partes interesadas pertinentes, en concreto a las partes usuarias de la cartera en lo que respecta a sus propios certificados, a los organismos de supervisión y a las autoridades de protección de datos competentes, solicitar la revocación de los certificados de registro de parte usuaria de la cartera;
 - g) la obligación de que el proveedor de certificados de registro de parte usuaria de la cartera registre todas esas revocaciones en su base de datos de certificados y publique el estado de revocación del certificado a su debido tiempo, y en cualquier caso en un plazo de veinticuatro horas a partir de la recepción de la solicitud de revocación;
 - h) la obligación de que los proveedores de certificados de registro de parte usuaria de la cartera faciliten información sobre el estado de validez o revocación de los certificados de registro de parte usuaria de la cartera que hayan expedido;
 - i) una descripción, cuando proceda, del modo en que un proveedor de certificados de registro de parte usuaria de la cartera archiva todos los certificados de registro de parte usuaria de la cartera que ha expedido;
 - j) la obligación de que los certificados de registro de parte usuaria de la cartera incluyan:
 - la ubicación en la que estén disponibles los datos de validación de la firma electrónica avanzada o del sello electrónico avanzado del certificado utilizado para firmar o sellar el certificado de registro, para toda la cadena de confianza que debe construirse hasta el ancla de confianza prevista;
 - una referencia legible por máquina a la política de certificación y la declaración de prácticas de certificación aplicables;
 - la información a que se refiere el anexo I, puntos 1, 2, 3, 5, 6 y 8, 9, 10, 11, 12, 13, 14 y 15;
 - la URL a la política de privacidad a que se refiere el artículo 8, apartado 2, letra g);
 - la política general de acceso a que se refiere el artículo 8, apartado 3.
4. El formato de intercambio de datos para el certificado de registro de parte usuaria se firmará con JSON Web Tokens (IETF RFC 7519) y CBOR Web Tokens (IETF RFC 8392).
5. La revocación mencionada en el punto 3, letra (g), será efectiva inmediatamente después de su publicación.
6. La información mencionada en el punto 3, letra (h), deberá proporcionarse al menos por cada certificado en cualquier momento, y al menos con posterioridad al período de validez del certificado, en un formato automatizado que sea fiable, gratuito y efectivo de conformidad con la política de certificación.