2024/2979

4.12.2024

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

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 *bis*, apartado 23,

Considerando lo siguiente:

(1) El marco europeo de identidad digital establecido por el Reglamento (UE) n.º 910/2014 es un componente crucial para la creación de un ecosistema de identidad digital seguro e interoperable en toda la Unión. El objetivo de este marco, con las carteras europeas de identidad digital (en lo sucesivo, «carteras») como piedra angular, es facilitar el acceso a los servicios en todos los Estados miembros, para las personas físicas y jurídicas, garantizando al mismo tiempo la protección de los datos personales y de la privacidad.

(2) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([2]) y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([3]) se aplican a todas las actividades de tratamiento de datos personales en virtud del presente Reglamento.

(3) El artículo 5 *bis*, apartado 23, del Reglamento (UE) n.º 910/2014 encomienda a la Comisión que, en caso necesario, establezca las especificaciones y los procedimientos pertinentes. Este mandato se lleva a cabo mediante cuatro Reglamentos de Ejecución, que tratan respectivamente de los protocolos y las interfaces: Reglamento de Ejecución (UE) 2024/2982 de la Comisión ([4]), la integridad y las funcionalidades básicas: Reglamento de Ejecución (UE) 2024/2979 de la Comisión ([5]), los datos de identificación de la persona y la declaración electrónica de atributos: Reglamento de Ejecución (UE) 2024/2977 de la Comisión ([6]), y las notificaciones a la Comisión: Reglamento de Ejecución (UE) 2024/2980 de la Comisión ([7]). El presente Reglamento establece los requisitos aplicables a la integridad y las funcionalidades básicas de las carteras europeas de identidad digital.

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

([2]) 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).

([3]) 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]) Reglamento de Ejecución (UE) 2024/2982 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 los protocolos y las interfaces que admitirá el marco europeo de identidad digital (DO L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) 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).

([6]) Reglamento de Ejecución (UE) 2024/2977 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 los datos de identificación de la persona y las declaraciones electrónicas de atributos expedidos a carteras europeas de identidad digital (DO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Reglamento de Ejecución (UE) 2024/2980 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 las notificaciones a la Comisión relativas al ecosistema de la cartera europea de identidad digital (DO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) 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 con arreglo a la 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 ([8]), y en particular la arquitectura y el marco de referencia. De conformidad con el considerando 75 del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo ([9]), la Comisión debe revisar y, en caso necesario, actualizar el presente Reglamento de Ejecución, para mantenerlo en consonancia con la evolución mundial, la arquitectura y el marco de referencia, y seguir las mejores prácticas en el mercado interior.

(5) A fin de garantizar una comunicación precisa, la diferenciación técnica y una asignación clara de responsabilidades, es necesario distinguir entre los distintos componentes y configuraciones de las carteras. Una solución de cartera debe entenderse como el sistema completo proporcionado por un proveedor de carteras que es necesario para que hacer que funcione una cartera, y debe comprender los componentes de *software* y de *hardware*, así como los servicios, ajustes y configuraciones necesarios para garantizar el correcto funcionamiento de la cartera. Una solución de cartera puede estar ubicada en los dispositivos y entornos de los usuarios o formar parte de la estructura lógica (*backend*) del proveedor. Una unidad de cartera debe entenderse como una configuración específica de la solución de cartera para un usuario individual, y debe comprender la aplicación instalada en el dispositivo o el entorno del usuario de una cartera con la que el usuario interactúa directamente (la «instancia de cartera») y las medidas de seguridad necesarias para proteger los datos y las transacciones del usuario. Estas medidas de seguridad deben incluir programas o equipos informáticos especiales para encriptar y proteger la información sensible. Una instancia de cartera debe formar parte de la unidad de cartera y permitir al usuario de una cartera acceder a las funcionalidades de esta.

(6) Las aplicaciones criptográficas seguras de cartera, como componentes especializados independientes dentro de una unidad de cartera, son necesarias no solo para la protección de los activos críticos, como las claves criptográficas privadas, sino también para el suministro de funcionalidades fundamentales, como la presentación de declaraciones electrónicas de atributos. El uso de especificaciones técnicas comunes puede facilitar el acceso de los proveedores de carteras a elementos seguros integrados. Las aplicaciones criptográficas seguras de cartera pueden proporcionarse de diversas maneras y para diversos tipos de dispositivos criptográficos seguros de cartera. Cuando los proveedores de carteras proporcionen aplicaciones criptográficas seguras de cartera personalizadas como *applets* de Java Card para elementos seguros integrados, deben seguir las normas indicadas en el anexo I o especificaciones técnicas equivalentes.

(7) Las unidades de cartera deben permitir a los proveedores de datos de identificación de la persona o declaraciones electrónicas de atributos verificar que están expidiendo estos datos o declaraciones a unidades de cartera auténticas del usuario de la cartera.

(8) Para garantizar la protección de datos mediante el diseño y por defecto, las carteras deben estar provistas de las técnicas de mejora de la privacidad más avanzadas disponibles. Estas características deben ofrecer la posibilidad de utilizar las carteras sin que el usuario de una cartera sea rastreable de unas partes usuarias de la cartera a otras, si esto es aplicable al caso de uso. Por ejemplo, los proveedores de carteras deben considerar las medidas de mitigación de la privacidad más avanzadas, como el uso de declaraciones efímeras de unidades de cartera o la expedición por lotes, en relación con las declaraciones de unidades de cartera. Además, las políticas de divulgación incorporadas deben prevenir a los usuarios de una cartera contra la divulgación inadecuada o ilegal de atributos a partir de las declaraciones electrónicas de atributos.

(9) Las declaraciones de unidades de cartera deben permitir a las partes usuarias de la cartera que soliciten atributos de las unidades de cartera verificar el estado de validez de la unidad de cartera con la que se están comunicando, ya que las declaraciones de unidad de cartera deben revocarse cuando una unidad de cartera ya no se considera válida. La información sobre el estado de validez de las unidades de cartera debe facilitarse de manera interoperable, de modo que pueda ser utilizada por todas las partes usuarias de la cartera. Además, en los casos en que los usuarios de una cartera hayan perdido sus unidades de cartera o ya no tengan control sobre ellas, los proveedores de carteras deben permitir que soliciten la revocación de su unidad de cartera. Para garantizar la privacidad y la no vinculación, los Estados miembros deben utilizar técnicas de protección de la privacidad también para la declaración de unidad de cartera. Pueden consistir en utilizar múltiples declaraciones de unidad de cartera para diferentes fines, revelando únicamente la información mínimamente pertinente sobre la cartera necesaria para una transacción, o en limitar la vida útil de la declaración de unidad de cartera como alternativa al uso de identificadores de revocación.

([8]) DO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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).

(10) A fin de garantizar que todas las carteras sean técnicamente capaces de recibir y presentar datos de identificación de la persona y declaraciones electrónicas de atributos en situaciones transfronterizas sin menoscabo de la interoperabilidad, las carteras deben admitir tipos predeterminados de formatos de datos y la divulgación selectiva. Como se establece en el Reglamento (UE) n.º 910/2014, la divulgación selectiva es un concepto que faculta al propietario de los datos para revelar solo determinadas partes de un conjunto de datos más amplio, a fin de que la entidad receptora obtenga únicamente la información que sea necesaria para la prestación de un servicio solicitado por el usuario. Puesto que las carteras deben permitir al usuario divulgar los atributos de manera selectiva, las normas enumeradas en el anexo II deben aplicarse de tal manera que hagan posible esta característica de las carteras. Además, pueden admitir otros formatos y funcionalidades que faciliten casos de uso específicos.

(11) El registro de las transacciones es una herramienta importante para proporcionar transparencia, al ofrecer una visión general de las transacciones al usuario de una cartera. Además, los registros deben utilizarse para poder compartir de manera rápida y fácil determinada información, a petición del usuario de una cartera, con las autoridades de control competentes establecidas de conformidad con el artículo 51 del Reglamento (UE) 2016/679, en caso de comportamiento sospechoso de las partes usuarias de la cartera.

(12) Para que el usuario de una cartera pueda firmar electrónicamente, debe expedírsele un certificado cualificado, que esté vinculado a un dispositivo de creación de firma electrónica cualificada. El usuario de una cartera debe tener acceso a una aplicación de creación de firma. Aunque la expedición de certificados cualificados es un servicio de proveedores de servicios de confianza cualificados, los proveedores de carteras u otras entidades deben poder proporcionar los demás componentes. Por ejemplo, los dispositivos de creación de firma electrónica cualificada pueden ser gestionados por los proveedores de servicios de confianza cualificados como un servicio o pueden estar localizados en el dispositivo del usuario de una cartera, como en una tarjeta inteligente. Del mismo modo, las aplicaciones de creación de firma pueden estar integradas en la instancia de cartera, pueden ser una aplicación independiente en el dispositivo del usuario de la cartera o pueden proporcionarse a distancia.

(13) Los objetos de exportación y portabilidad de datos pueden registrar los datos de identificación de la persona y las declaraciones electrónicas de atributos que se han expedido a una determinada unidad de cartera. Estos objetos permiten a los usuarios de una cartera extraer los datos pertinentes de su unidad de cartera con el fin de reforzar su derecho a la portabilidad de los datos. Se anima a los proveedores de carteras a que utilicen las mismas soluciones técnicas para ejecutar también procesos de copia de seguridad y recuperación de las unidades de cartera, que permitan recuperar aquellas que se pierdan o transferir información de un proveedor de cartera a otro, cuando proceda y en la medida en que esto pueda hacerse sin menoscabar el derecho a la protección de datos ni la seguridad del ecosistema de identidad digital.

(14) La generación de seudónimos específicos de las partes usuarias de la cartera debe permitir a los usuarios de las carteras autenticarse sin proporcionar a dichas partes información superflua. Tal como se establece en el Reglamento (UE) n.º 910/2014, no se debe impedir que los usuarios de la cartera accedan a los servicios con un seudónimo, cuando la normativa no exija una identidad jurídica para la autenticación. Por lo tanto, las carteras deben incluir una funcionalidad para generar seudónimos elegidos y gestionados por los usuarios, que les permitan autenticarse cuando accedan a los servicios en línea. La ejecución de las especificaciones establecidas en el anexo V debe permitir estas funcionalidades en consecuencia. Además, las partes usuarias de la cartera no deben solicitar a los usuarios que faciliten otros datos que no sean los indicados para el uso al que están destinadas las carteras en el registro de partes usuarias. Conviene que los usuarios de la cartera puedan verificar en cualquier momento los datos de registro de las partes usuarias.

(15) Tal como se establece en el Reglamento (UE) 2024/1183, los Estados miembros no deben limitar, directa ni indirectamente, el acceso a los servicios públicos o privados a personas físicas o jurídicas que no opten por utilizar carteras y deben facilitar otras soluciones adecuadas.

(16) 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 ([10]), emitió su dictamen el 30 de septiembre de 2024.

([10]) 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).

(17) Las medidas previstas en el presente Reglamento se ajustan al dictamen del comité contemplado en el artículo 48 del Reglamento (UE) n.º 910/2014.

HA ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

El presente Reglamento establece normas para la integridad y las funcionalidades básicas de las carteras, que deben actualizarse periódicamente para mantenerlas en consonancia con la evolución de la tecnología y las normas y con el trabajo realizado sobre la base de la Recomendación (UE) 2021/946, y en particular la arquitectura y el marco de referencia.

Artículo 2

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «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;

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 cartera a un usuario particular de una cartera;

3) «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;

4) «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;

5) «usuario de una cartera»: usuario que tiene el control sobre la unidad de cartera;

6) «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;

7) «proveedor de cartera»: persona física o jurídica que proporciona soluciones de cartera;

8) «declaración de unidad de cartera»: objeto de datos que describe los componentes de la unidad de cartera o permite la autenticación y la validación de esos componentes;

9) «política de divulgación incorporada»: conjunto de normas, incorporadas en una declaración electrónica de atributos por su proveedor, que indica las condiciones que debe cumplir una parte usuaria de la cartera para acceder a la declaración electrónica de atributos;

10) «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;

11) «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;

12) «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;

13) «operación criptográfica de una cartera»: mecanismo criptográfico necesario en el contexto de la autenticación del usuario de una cartera y la expedición o presentación de datos de identificación de la persona o declaraciones electrónicas de atributos;

14) «certificado de acceso de partes usuarias de la cartera»: certificado para sellos o firmas electrónicos, expedido por un proveedor de certificados de acceso de partes usuarias de la cartera, que autentica y valida a la parte usuaria de la cartera;

15) «proveedor de certificados de acceso de partes usuarias de la cartera»: persona física o jurídica a la que un Estado miembro ha encomendado expedir certificados de acceso de parte usuaria a las partes usuarias de cartera registradas en ese Estado miembro.

CAPÍTULO II

INTEGRIDAD DE LAS CARTERAS EUROPEAS DE IDENTIDAD DIGITAL

Artículo 3

Integridad de la unidad de cartera

1. Las unidades de cartera no llevarán a cabo ninguna de las funciones enumeradas en el artículo 5 *bis*, apartado 4, del Reglamento (UE) n.º 910/2014, excepto la autenticación del usuario de una cartera para acceder a la unidad de cartera, hasta que la unidad de cartera haya autenticado correctamente al usuario de la cartera.

2. Para cada unidad de cartera, los proveedores de carteras firmarán o sellarán al menos una declaración de unidad de cartera que cumpla los requisitos establecidos en el artículo 6. El certificado utilizado para firmar o sellar la declaración de unidad de cartera se expedirá con arreglo a un certificado incluido en la lista de confianza a que se refiere el Reglamento de Ejecución (UE) 2024/2980.

Artículo 4

Instancias de cartera

1. Las instancias de cartera utilizarán al menos un dispositivo criptográfico seguro de cartera para gestionar los activos críticos.

2. Los proveedores de carteras garantizarán la integridad, autenticidad y confidencialidad de la comunicación entre las instancias de cartera y las aplicaciones criptográficas seguras de cartera.

3. Cuando los activos críticos estén relacionados con la realización de una identificación electrónica a un nivel de seguridad alto, las operaciones criptográficas de la cartera u otras operaciones de tratamiento de activos críticos se llevarán a cabo conforme a los requisitos aplicables a las características y el diseño de los medios de identificación electrónica con un nivel de seguridad alto, tal como se establece en el Reglamento de Ejecución (UE) 2015/1502 de la Comisión ([11]).

Artículo 5

Aplicaciones criptográficas seguras de cartera

1. Los proveedores de carteras garantizarán que las aplicaciones criptográficas seguras de cartera:

a) únicamente lleven a cabo operaciones criptográficas de cartera que impliquen activos críticos distintos de los necesarios para que la unidad de cartera autentique al usuario de la cartera en casos en que dichas aplicaciones hayan autenticado correctamente a los usuarios de la cartera;

([11]) 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).

b) cuando autentiquen a los usuarios de una cartera en el contexto de la realización de una identificación electrónica con un nivel de seguridad alto, realicen la autenticación de los usuarios de una cartera con arreglo a los requisitos aplicables a las características y al diseño de medios de identificación electrónica con un nivel de seguridad alto, tal como se establece en el Reglamento de Ejecución (UE) 2015/1502;

c) sean capaces de generar de manera segura nuevas claves criptográficas;

d) sean capaces de suprimir de manera segura activos críticos;

e) sean capaces de generar una prueba de posesión de claves privadas;

f) protejan las claves privadas generadas por esas aplicaciones criptográficas seguras de cartera mientras existan esas claves;

g) cumplan los requisitos aplicables a las características y el diseño de los medios de identificación electrónica a un nivel de seguridad alto, tal como se establece en el Reglamento de Ejecución (UE) 2015/1502;

h) sean los únicos componentes capaces de ejecutar operaciones criptográficas de cartera y cualquier otra operación con activos críticos en el contexto de la realización de una identificación electrónica a un nivel de seguridad alto.

2. Cuando los proveedores de carteras decidan proporcionar una aplicación criptográfica segura de cartera a un elemento seguro integrado, basarán su solución técnica en las especificaciones técnicas enumeradas en el anexo I u otras especificaciones técnicas equivalentes.

Artículo 6

Autenticidad y validez de la unidad de cartera

1. Los proveedores de carteras se asegurarán de que cada unidad de cartera contenga declaraciones de unidad de cartera.

2. Los proveedores de carteras se asegurarán de que las declaraciones de unidad de cartera a que se refiere el apartado 1 contengan claves públicas y de que las claves privadas correspondientes estén protegidas por un dispositivo criptográfico seguro de cartera.

3. Los proveedores de carteras:

a) informarán a los usuarios de una cartera de sus derechos y obligaciones en relación con su unidad de cartera;

b) proporcionarán mecanismos, independientes de las unidades de cartera, para la identificación y autenticación seguras de los usuarios de una cartera;

c) garantizarán que los usuarios de una cartera tengan derecho a solicitar la revocación de sus declaraciones de unidad de cartera, utilizando los mecanismos de autenticación a que se refiere la letra b).

Artículo 7

Revocación de las declaraciones de unidad de cartera

1. Los proveedores de carteras serán las únicas entidades capaces de revocar las declaraciones de unidad de cartera que ellos hayan suministrado.

2. Los proveedores de carteras establecerán y harán pública una política en la que se especifiquen las condiciones y los plazos para la revocación de las declaraciones de unidad de cartera.

3. Cuando los proveedores de carteras hayan revocado declaraciones de unidad de cartera, informarán a los usuarios de una cartera afectados en un plazo de veinticuatro horas a partir de la revocación de sus unidades de cartera, indicando el motivo de la revocación y las consecuencias para el usuario de una cartera. Esta información se transmitirá de manera concisa, fácilmente accesible y mediante un lenguaje claro y sencillo.

4. Cuando los proveedores de carteras hayan revocado declaraciones de unidad de cartera, harán público el estado de validez de la declaración de unidad de cartera, de manera que se preserve la privacidad, y describirán la ubicación de esa información en la declaración de unidad de cartera.

CAPÍTULO III

FUNCIONALIDADES Y CARACTERÍSTICAS BÁSICAS DE LAS CARTERAS EUROPEAS DE IDENTIDAD DIGITAL

Artículo 8

Formatos para los datos de identificación de la persona y las declaraciones electrónicas de atributos

Los proveedores de carteras se asegurarán de que las soluciones de cartera admitan el uso de datos de identificación de la persona y declaraciones electrónicas de atributos expedidos de conformidad con la lista de normas que figura en el anexo II.

Artículo 9

Registros de las transacciones

1. Con independencia de que una transacción se haya concluido efectivamente o no, las instancias de cartera registrarán todas las transacciones realizadas con partes usuarias de la cartera y otras unidades de cartera, incluidos la firma y el sello electrónicos.

2. La información registrada contendrá, como mínimo:

a) la fecha y la hora de la transacción;

b) el nombre, los datos de contacto y el identificador único de la parte usuaria de la cartera correspondiente y el Estado miembro en el que esté establecida dicha parte, o, en el caso de otras unidades de cartera, la información pertinente de la declaración de unidad de cartera;

c) el tipo o los tipos de datos solicitados y presentados en la transacción;

d) en el caso de las transacciones no concluidas, el motivo de esa inconclusión.

3. Los proveedores de carteras garantizarán la integridad, la autenticidad y la confidencialidad de la información registrada.

4. Las instancias de cartera registrarán los informes enviados por el usuario de una cartera a las autoridades de protección de datos a través de su unidad de cartera.

5. El proveedor de cartera tendrá acceso a los registros a que se refieren los apartados 1 y 2 cuando sea necesario para la prestación de servicios de cartera y con el consentimiento previo explícito del usuario de una cartera.

6. Los registros a que se refieren los apartados 1 y 2 seguirán siendo accesibles mientras así lo exijan el Derecho de la Unión o el Derecho nacional.

7. Los proveedores de carteras permitirán a los usuarios de una cartera exportar la información registrada a que se refiere el apartado 2.

Artículo 10

Divulgación incorporada

1. Los proveedores de carteras se asegurarán de que las unidades de cartera que proporcionen puedan procesar las declaraciones electrónicas de atributos con las políticas de divulgación incorporada comunes establecidas en el anexo III.

2. Las instancias de cartera podrán procesar y presentar las políticas de divulgación incorporada a que se refiere el apartado 1 junto con los datos recibidos de la parte usuaria de la cartera solicitante.

3. Las instancias de cartera verificarán si la parte usuaria de la cartera cumple los requisitos de la política de divulgación incorporada e informarán al usuario de una cartera del resultado.

Artículo 11

Firmas electrónicas cualificadas y sellos electrónicos cualificados

1. Los proveedores de carteras garantizarán que los usuarios de una cartera puedan recibir certificados cualificados para firmas electrónicas cualificadas o sellos electrónicos cualificados que estén vinculados a dispositivos de creación de firma o sello cualificados que sean locales, externos o a distancia en relación con las instancias de cartera.

2. Los proveedores de carteras se asegurarán de que las soluciones de cartera puedan interactuar de forma segura con uno de los siguientes tipos de dispositivos de creación de firma o sello cualificados: dispositivos locales, externos o gestionados a distancia de creación de firma o sello cualificados con la finalidad de utilizar los certificados cualificados a que se refiere el apartado 1.

3. Los proveedores de carteras se asegurarán de que los usuarios de una cartera que sean personas físicas tengan, al menos para los fines no profesionales, acceso gratuito a aplicaciones de creación de firma que permitan crear firmas electrónicas cualificadas gratuitas utilizando los certificados a que se refiere el apartado 1.

Artículo 12

Aplicaciones de creación de firma

1. Las aplicaciones de creación de firma utilizadas por las unidades de cartera podrán ser facilitadas por los proveedores de carteras, por los proveedores de servicios de confianza o por las partes usuarias de la cartera.

2. Las aplicaciones de creación de firma tendrán las siguientes funciones:

a) firmar o sellar los datos facilitados por el usuario de una cartera;

b) firmar o sellar los datos facilitados por las partes usuarias;

c) crear firmas o sellos que sean conformes, como mínimo, con los formatos obligatorios a que se refiere el anexo IV;

d) informar a los usuarios de una cartera sobre el resultado del proceso de creación de la firma o el sello.

3. Las aplicaciones de creación de firma podrán estar integradas en las instancias de cartera o ser externas a ellas. Cuando las aplicaciones de creación de firma se basen en dispositivos de creación de firma cualificada a distancia y cuando estén integradas en instancias de cartera, admitirán la interfaz de programación de aplicaciones a que se refiere el anexo IV.

Artículo 13

Exportación y portabilidad de los datos

Cuando sea técnicamente viable, y salvo que se trate de activos críticos, las unidades de cartera darán soporte a la exportación y la portabilidad seguras de los datos personales del usuario de una cartera, a fin de que este pueda migrar a una unidad de cartera de una solución de cartera diferente de un modo que garantice un nivel de seguridad alto según lo establecido en el Reglamento de Ejecución (UE) 2015/1502.

Artículo 14

Seudónimos

1. Las unidades de cartera admitirán la generación de seudónimos para los usuarios de una cartera de conformidad con las especificaciones técnicas establecidas en el anexo V.

2. Las unidades de cartera admitirán la generación, cuando una parte usuaria de la cartera así lo solicite, de un seudónimo específico y exclusivo para ella, y se lo facilitarán por sí solo o junto con los datos de identificación de la persona o la declaración electrónica de atributos que dicha parte usuaria de la cartera haya solicitado.

CAPÍTULO IV

DISPOSICIONES FINALES

Artículo 15

Entrada en vigor

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

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

Hecho en Bruselas, el 28 de noviembre de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

LISTA DE NORMAS A QUE SE REFIERE EL ARTÍCULO 5

— SAM.01 Secured Applications for Mobile-Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;

— GPCon GUI_ 217 GlobalPlatform SAM Configuration Technical Speciation for implementation of SAM v1.0 2024-04;

— GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;

— GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;

— GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;

— GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;

— GPD_SPE_0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

ANEXO II

LISTA DE NORMAS A QUE SE REFIERE EL ARTÍCULO 8

— ISO/IEC.18013-5:2021

— «Modelo de datos de credenciales verificables 1.1», recomendación del W3C, de 3 de marzo de 2022.

ANEXO III

LISTA DE LAS POLÍTICAS DE DIVULGACIÓN INCORPORADA A QUE SE REFIERE EL ARTÍCULO 10

1. «Ninguna política»: indica que no se aplica ninguna política a las declaraciones electrónicas de atributos.
2. «Política de solo partes usuarias autorizadas»: indica que los usuarios de una cartera únicamente pueden divulgar las declaraciones electrónicas de atributos a las partes usuarias autenticadas que se mencionen explícitamente en las políticas de divulgación.
3. «Raíz de confianza específica»: indica que los usuarios de una cartera únicamente deben divulgar la declaración electrónica de atributos específica a las partes usuarias de la cartera autenticadas con certificados de acceso de parte usuaria de la cartera derivados de una raíz específica (o una lista de raíces específicas) o con certificados intermedios.

ANEXO IV

FORMATOS DE FIRMA Y SELLO A QUE SE REFIERE EL ARTÍCULO 12

1. Formato obligatorio de firma o sello:

   a) PAdES (firma electrónica avanzada PDF), tal como se especifica en la norma del ETSI EN 319 142-1 V1.1.1 (2016-04); firmas electrónicas e infraestructuras (ESI); firmas digitales PAdES; parte 1: Componentes elementales y firmas básicas PAdES.

2. Lista de formatos opcionales de firma o sello:

   a) XAdES, tal como se especifica en la norma del ETSI EN 319 132-1 V1.2.1 (2022-02) firmas electrónicas e infraestructuras (ESI); firmas digitales XAdES; parte 1: Componentes elementales y firmas básicas XAdES (XAdES) para la firma en formato XML;

   b) JAdES, tal como se especifica en la norma del ETSI TS 119 182-1 V1.2.1 (2024-07) firmas electrónicas e infraestructuras (ESI); firmas digitales JAdES; parte 1: Componentes elementales y firmas básicas XAdES (XAdES) para la firma en formato JSON;

   c) CAdES (firma electrónica avanzada CMS) tal como se especifica en la norma del ETSI EN 319 122-1 V1.3.1 (2023-06) firmas electrónicas e infraestructuras (ESI); firmas digitales CAdES; parte 1: Componentes elementales y firmas básicas CAdES para la firma en formato CMS;

   d) ASiC (contenedor de firmas asociadas), tal como se especifica en la norma del ETSI EN 319 162-1 V1.1.1 (2016-04) firmas electrónicas e infraestructuras (ESI); contenedores de firmas asociadas (ASiC); parte 1: Componentes elementales y contenedores ASiC de base y norma del ETSI EN 319 162-2 V1.1.1 (2016-04) firmas electrónicas e infraestructuras (ESI); contenedores de firmas asociadas (ASiC); parte 2: contenedores ASiC adicionales para la firma de contenedores.

3. Interfaz de programación de aplicaciones:

   — Especificación del consorcio de firmas en la nube (CSC) v2.0 (20 de abril de 2023).

ANEXO V

ESPECIFICACIONES TÉCNICAS PARA LA GENERACIÓN DE SEUDÓNIMOS A QUE SE REFIERE EL ARTÍCULO 14

Especificaciones técnicas:

— WebAuthn – recomendación del W3C, de 8 de abril de 2021, nivel 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.