2026/1731

22.7.2026

REGLAMENTO DE EJECUCIÓN (UE) 2026/1731 DE LA COMISIÓN

de 15 de julio de 2026

por el que se modifican los Reglamentos de Ejecución (UE) 2024/2977, (UE) 2024/2979, (UE) 2024/2980 y (UE) 2024/2982 en lo que respecta a las normas y especificaciones aplicables

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE ([1]), y en particular su artículo 5 *bis*, apartado 23,

Considerando lo siguiente:

(1) Con el fin de garantizar el máximo nivel de armonización entre los Estados miembros para el desarrollo de las carteras europeas de identidad digital, las especificaciones técnicas se basan en el trabajo realizado con arreglo a la Recomendación (UE) 2021/946 de la Comisión ([2]), y en particular la arquitectura y el marco de referencia. Dado que la arquitectura y el marco de referencia han evolucionado significativamente desde los Reglamentos de Ejecución (UE) 2024/2977 ([3]), (UE) 2024/2979 ([4]), (UE) 2024/2980 ([5]) y (UE) 2024/2982 ([6]) de la Comisión, dichos Reglamentos de Ejecución deben modificarse ahora para adaptarlos a las nuevas normas, especificaciones y procedimientos.

De conformidad con los objetivos del Reglamento (UE) n.º 910/2014, se han seleccionado una serie de normas para cumplir estos requisitos específicos. Estas normas deben reflejar las prácticas establecidas y ser ampliamente aceptadas en los sectores pertinentes. Por ejemplo, dado que el formato VCDM del W3C se utiliza como formato de referencia para las certificaciones, en particular en el sector educativo, las carteras europeas de identidad digital también deben admitir este formato cuando estén disponibles los nuevos perfiles en dicho formato. Cuando sea necesario, estas normas deben adaptarse o complementarse para garantizar la seguridad y fiabilidad de las carteras europeas de identidad digital, facilitando al mismo tiempo la interoperabilidad transfronteriza y el funcionamiento eficaz del mercado interior.

(2) Para cualquier uso de la cartera que requiera la presentación del retrato del usuario de la cartera, las soluciones de cartera deben permitir la funcionalidad de divulgación selectiva y la divulgación debe estar bajo el control pleno del usuario. Para proteger la capacidad de decidir sobre la divulgación y proteger el retrato frente a una solicitud de divulgación no intencionada o no autorizada, el diseño arquitectónico de las carteras europeas de identidad digital debe prever mecanismos de alerta y registrar todas las transacciones relacionadas con el uso del retrato. Para garantizar que el usuario de una cartera sea consciente de que va a compartir datos biométricos, las advertencias deben indicar que la solicitud implica el intercambio de datos biométricos y exigir específicamente al usuario que

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

([2]) Recomendación (UE) 2021/946 de la Comisión, de 3 de junio de 2021, sobre un conjunto de instrumentos común de la Unión para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea (DO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Reglamento de Ejecución (UE) 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).

([4]) 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).

([5]) Reglamento de Ejecución (UE) 2024/2980, de 28 de noviembre de 2024, de la Comisión, 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).

([6]) 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).

confirme su divulgación. Cuando una parte usuaria trate el retrato con el fin de identificar de manera unívoca a una persona física o de confirmar la identidad alegada de dicha persona, se aplicarán el artículo 6 y 9 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([7]), así como todos los demás requisitos de dicho Reglamento, en particular que el tratamiento del retrato por las partes usuarias debe limitarse a lo necesario para el uso previsto. El uso previsto debe comunicarse al usuario de la cartera, junto con la solicitud de divulgación, en un lenguaje claro e inteligible. Para tener debidamente en cuenta la sensibilidad de los datos biométricos, el usuario de una cartera debe confirmar explícita y específicamente la divulgación del retrato. El silencio o las casillas marcadas previamente no deben considerarse confirmación por parte del usuario de la cartera. La confirmación explícita del usuario de una cartera debe ser una salvaguardia técnica y no proporcionar en sí misma un fundamento jurídico para el tratamiento. Como se establece en el artículo 9, apartado 4, del Reglamento (UE) 2016/679 «[l]os Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud».

(3) A fin de que los Estados miembros dispongan de tiempo suficiente para adaptar sus procedimientos nacionales, el retrato del usuario de una cartera solo puede formar parte de los datos obligatorios de identificación de la persona física a partir del 11 de agosto de 2028. Cuando estas imágenes se obtengan de documentos de identidad existentes, como documentos de identidad o pasaportes, se aplicarán los requisitos pertinentes establecidos respectivamente en los Reglamentos (UE) 2025/1208 ([8]) o (CE) n.º 2252/2004 ([9]) del Consejo.

(4) El Reglamento (UE) n.º 910/2014 exige que las carteras puedan mostrar una etiqueta de confianza de la UE para la cartera de identidad digital como indicación verificable, sencilla y reconocible de que una cartera se ha proporcionado de conformidad con el Reglamento. El uso de esta etiqueta de confianza contribuirá al funcionamiento eficaz del mercado interior, garantizará la competencia leal y protegerá los intereses de los consumidores. Para permitir el uso de dicha etiqueta de confianza, deben establecerse sus características visuales y técnicas.

(5) Tal como se establece en el artículo 12 *ter* del Reglamento (UE) n.º 910/2014, los guardianes de acceso deben permitir a los proveedores de carteras europeas de identidad digital y a los emisores de medios de identificación electrónica notificados la interoperabilidad efectiva con las mismas características de sistema operativo, de equipo (*hardware*) o de programa informático (*software*) y, a efectos de interoperabilidad, el acceso a ellas. Dicha interoperabilidad y acceso efectivos deben proporcionarse de forma gratuita y con independencia de si dichas características de *hardware* o *software* forman parte del sistema operativo, están a disposición de dicho guardián de acceso o son utilizadas por este al prestar tales servicios. Dado que todas las soluciones de cartera deben apoyar un conjunto común de protocolos e interfaces para garantizar la usabilidad, la seguridad y la interoperabilidad en todos los Estados miembros, los guardianes de acceso deben permitir las características del sistema operativo, el *hardware* o el *software* necesarias para aplicar los protocolos e interfaces establecidos en el anexo XII del presente Reglamento. En este contexto, en los flujos en línea entre dispositivos, tanto para el control físico de proximidad como para la transferencia de datos entre los dos dispositivos, los guardianes de acceso deben preferir un canal de comunicación local, habilitado por la versión 2.3 de la especificación del Client to Authenticator Protocol (CTAP) ([10]), a utilizar los servicios del túnel híbrido del CTAP.

(6) A fin de que los Estados miembros, los proveedores de certificados de registro de partes usuarias de la cartera y los proveedores de carteras dispongan de tiempo suficiente para que las unidades de cartera puedan autenticar y validar los certificados de registro de partes usuarias de la cartera, este requisito solo debe aplicarse a partir del 11 de agosto de 2028.

(7) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([11]) son aplicables a las actividades de tratamiento de datos personales en virtud del presente Reglamento.

([7]) 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).

([8]) Reglamento (UE) 2025/1208 del Consejo, de 12 de junio de 2025, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación (DO L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Reglamento (CE) n.º 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros (DO L 385 de 29.12.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Norma propuesta por la Fido Alliance, Client to Authenticator Protocol (CTAP), 26 de febrero de 2026.

([11]) 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) 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 ([12]), emitió su dictamen el 17 de abril de 2026 ([13]).

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

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Modificaciones del Reglamento de Ejecución (UE) 2024/2977

El Reglamento de Ejecución (UE) 2024/2977 se modifica como sigue:

1) Se inserta el artículo 3 *bis* siguiente:

«*Artículo 3* bis

Protección del retrato

1. Además de los requisitos de información en virtud del Reglamento (UE) 2016/679, los proveedores de carteras se asegurarán de que las soluciones de cartera que ofrezcan emitan advertencias a los usuarios de una cartera cuando las partes usuarias soliciten la divulgación del retrato, indicando que la solicitud implica el intercambio de datos biométricos y que requiere la confirmación de la divulgación selectiva del retrato.

2. Para la aplicación de la divulgación selectiva del retrato a una parte usuaria de la cartera, los proveedores de carteras garantizarán que las soluciones de cartera exijan que el usuario de la cartera confirme explícita y específicamente la presentación del retrato.

3. El retrato no será conservado por las partes usuarias de la cartera a menos que su tratamiento sea necesario a efectos de identificación y autenticación de conformidad con el Derecho de la Unión en materia de protección de datos o cuando así lo disponga el Derecho de la Unión o nacional, de conformidad con el Derecho de la Unión en materia de protección de datos. El retrato no se transferirá a terceros países u organizaciones internacionales a menos que lo permita el Derecho de la Unión en materia de protección de datos.».

2) En el artículo 4, el apartado 1 se sustituye por el texto siguiente:

«1. Las declaraciones electrónicas de atributos expedidas a unidades de cartera cumplirán al menos una de las normas establecidas en el anexo II del Reglamento de Ejecución (UE) 2024/2979.».

3) En el artículo 5, apartado 4, la letra b) se sustituye por el texto siguiente:

«b) cuando se haya revocado la declaración de unidad de cartera de la unidad de cartera a la que se expidieron los datos de identificación de la persona;»;

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

([12]) 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).

([13]) Observaciones formales del SEPD sobre el proyecto de Reglamento de Ejecución en lo que respecta a las normas y especificaciones aplicables y por el que se corrige el Reglamento de Ejecución (UE) 2024/2980 | Supervisor Europeo de Protección de Datos.

Artículo 2

Modificaciones del Reglamento de Ejecución (UE) 2024/2979

El Reglamento de Ejecución (UE) 2024/2979 se modifica como sigue:

1) En el artículo 3 se suprime el apartado 2.

2) En el artículo 5, apartado 1, la letra a) se sustituye por el texto siguiente:

«a) lleven a cabo operaciones criptográficas de cartera que impliquen activos almacenados en un dispositivo criptográfico seguro de cartera y que no sean necesarios para la autenticación del usuario de la cartera únicamente en aquellos casos en que dichas aplicaciones hayan autenticado correctamente a los usuarios de la cartera;».

3) Se inserta el artículo 5 *bis* siguiente:

«*Artículo 5* bis

Mecanismos criptográficos

A efectos del artículo 4, apartado 2, los proveedores de carteras utilizarán únicamente los mecanismos criptográficos a que se refiere el anexo I *bis*.».

4) El artículo 6 se modifica como sigue:

a) El apartado 1 se sustituye por el texto siguiente:

«1. Los proveedores de carteras expedirán declaraciones de unidad de cartera para cada unidad de cartera. Los proveedores de carteras firmarán o sellarán las declaraciones de unidad de cartera de manera que las firmas o sellos puedan validarse mediante un certificado enumerado de conformidad con el anexo II, sección 2, punto 1, letra h), del Reglamento de Ejecución (UE) 2024/2980.».

b) El apartado 2 se sustituye por el texto siguiente:

«2. Los proveedores de carteras velarán por que las declaraciones de unidad de cartera a que se refiere el apartado 1 cumplan las especificaciones técnicas establecidas en el anexo I *ter*.».

c) En el apartado 3, la letra b) se sustituye por el texto siguiente:

«b) proporcionarán mecanismos seguros de identificación y autenticación de los usuarios de una cartera que sean independientes de las unidades de cartera;».

5) En el artículo 9, apartado 2, la letra b) se sustituye por el texto siguiente:

«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;».

6) En el artículo 10, el apartado 1 se sustituye por el texto siguiente:

«1. Los proveedores de carteras se asegurarán de que las unidades de cartera que proporcionen puedan procesar las declaraciones electrónicas de atributos expedidas con arreglo a las especificaciones técnicas aplicables para las políticas de divulgación incorporadas comunes establecidas en el anexo III.».

7) El artículo 12 se modifica como sigue:

a) En el apartado 2, la letra c) se sustituye por el texto siguiente:

«c) crear firmas o sellos que sean conformes, como mínimo, con el formato obligatorio de firma o sello a que se refiere el anexo IV.».

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

«3. Las aplicaciones de creación de firma podrán estar integradas en las instancias de cartera o ser externas a ellas.».

c) Se inserta el apartado siguiente:

«4. Las aplicaciones de creación de firma utilizadas por las unidades de cartera admitirán, como mínimo, la interfaz de programación de aplicaciones a que se refiere el anexo IV.».

8) En el artículo 14 se suprime el apartado 1.

9) Se inserta el artículo 14 *bis* siguiente:

«*Artículo 14* bis

Etiqueta de confianza de la UE para la cartera de identidad digital

1. Los proveedores de carteras se asegurarán de que las unidades de cartera muestren la etiqueta de confianza de la UE para la cartera de identidad digital. La etiqueta de confianza de la UE para la cartera de identidad digital adoptará la forma establecida en los anexos VI y VII.

2. Los proveedores de carteras se asegurarán de que las unidades de cartera permitan a los usuarios de una cartera acceder a información que les permita verificar el estado de certificación de la solución de cartera. A tal fin, los proveedores de carteras se asegurarán de que, tras el registro de una solución de cartera, las unidades de cartera correspondientes incluyan las URL facilitadas por la Comisión Europea para tal verificación. Los proveedores de carteras velarán por que sus unidades de cartera tengan acceso a datos de la etiqueta de confianza de la UE para la cartera de identidad digital que cumplan las especificaciones técnicas establecidas en el anexo VIII.

3. Los colores de referencia para la etiqueta de confianza de la UE para la cartera de identidad digital serán Pantone n.º 661 y 116, o azul (100 % cian + 67 % magenta + 0 % amarillo + 40 % negro) y amarillo (0 % cian + 20 % magenta + 100 % amarillo + 0 % negro), cuando se utilice la cuatricromía; cuando se utilicen colores RGB, la referencia será azul (0 rojo + 51 verde + 153 azul) y amarillo (255 rojo + 204 verde + 0 azul).

4. La etiqueta de confianza de la UE para la cartera de identidad digital podrá utilizarse en blanco y negro, tal como se establece en el anexo VII, solamente cuando el uso del color no sea posible.

5. Cuando la etiqueta de confianza de la cartera de identidad digital de la UE se utilice sobre un fondo oscuro, podrá utilizarse en formato negativo utilizando el mismo color de fondo. Cuando la etiqueta de confianza de la cartera de identidad digital de la UE se utilice en color sobre un fondo de color que dificulte su visualización, podrá utilizarse una línea de delimitación en torno a dicha etiqueta para mejorar el contraste con los colores de fondo.

6. La etiqueta de confianza de la UE para la cartera de identidad digital tendrá un tamaño mínimo de 64 × 85 píxeles, con 150 ppp (puntos por pulgada).

7. Los proveedores de carteras velarán por que la etiqueta de confianza de la UE para la cartera de identidad digital se utilice de manera que permita indicar claramente la unidad de cartera a la que pertenece la etiqueta de confianza de la UE para la cartera de identidad digital. La etiqueta de confianza de la UE para la cartera de identidad digital podrá asociarse a elementos gráficos o textuales que indiquen claramente la unidad de cartera para la que se utiliza, siempre que no modifiquen su capacidad de ser reconocida como etiqueta de confianza de la UE para la cartera de identidad digital, ni alteren la asociación con la lista de carteras europeas de identidad digital certificadas a que se refiere el artículo 5 *quinquies* del Reglamento (UE) n.º 910/2014.

8. Cuando los proveedores de carteras hayan revocado una declaración de unidad de cartera, velarán por que la unidad de cartera correspondiente deje de mostrar la etiqueta de confianza de la UE para la cartera de identidad digital.».

10) Se añaden los anexos I *bis* y I *ter* que figuran en los anexos II y III del presente Reglamento.

11) El anexo II se sustituye por el anexo IV del presente Reglamento.

12) El anexo III se sustituye por el anexo V del presente Reglamento.

13) El anexo IV se modifica de conformidad con el anexo VI del presente Reglamento.

14) Se suprime el anexo V.

15) Se inserta como anexo VI el texto que figura en el anexo VII del presente Reglamento.

16) Se inserta como anexo VII el texto establecido en el anexo VIII del presente Reglamento.

17) Se inserta como anexo VIII el texto establecido en el anexo IX del presente Reglamento.

Artículo 3

Modificaciones del Reglamento de Ejecución (UE) 2024/2980

El Reglamento de Ejecución (UE) 2024/2980 se modifica como sigue:

1) En el artículo 5, el apartado 2 se sustituye por el texto siguiente:

«2. En su caso, la Comisión establecerá, mantendrá y publicará una lista en la que se recopilará la información notificada por los Estados miembros sobre los proveedores de carteras, los proveedores de datos de identificación de la persona, los proveedores de certificados de acceso de partes usuarias de la cartera y los proveedores de certificados de registro de partes usuarias de la cartera a que se refieren las secciones 2, 3, 4 y 5 del anexo II.».

2) El anexo II del Reglamento de Ejecución (UE) 2024/2980 se modifica de conformidad con el anexo X del presente Reglamento.

Artículo 4

Modificaciones del Reglamento de Ejecución (UE) 2024/2982

El Reglamento de Ejecución (UE) 2024/2982 se modifica como sigue:

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

«2) la presentación de atributos de los datos de identificación de la persona y las declaraciones electrónicas de atributos a las partes usuarias de la cartera;».

2) El artículo 3 se modifica como sigue:

a) El apartado 1 se sustituye por el texto siguiente:

«1) autentiquen y validen los certificados de acceso de la parte usuaria de la cartera cuando interactúen con partes usuarias de la cartera sin delegar la ejecución de estos procesos en un navegador del sistema operativo u otra aplicación intermediaria;».

b) Se suprime el apartado 2.

c) El apartado 3 se sustituye por el texto siguiente:

«3) autentiquen y validen las solicitudes realizadas utilizando certificados de acceso de parte usuaria de la cartera;».

d) El apartado 4 se sustituye por el texto siguiente:

«4) autentiquen y validen el certificado de registro de la parte usuaria de la cartera;».

e) El apartado 5 se sustituye por el texto siguiente:

«5) muestren a los usuarios de una cartera la información contenida en los certificados de acceso de la parte usuaria de la cartera;».

f) Se suprime el apartado 8.

g) El apartado 9 se sustituye por el texto siguiente:

«9) no presenten ningún atributo solicitado a las partes usuarias de la cartera hasta que se hayan completado los pasos siguientes:

a) la verificación de que las políticas de divulgación incorporadas hayan sido procesadas en la unidad de cartera de conformidad con el artículo 10 del Reglamento de Ejecución (UE) 2024/2979;

b) la verificación de que los usuarios de una cartera hayan aprobado total o parcialmente la presentación;».

3) En el artículo 4, el apartado 1 se sustituye por el texto siguiente:

«1. Los proveedores de carteras se asegurarán de que las soluciones de cartera admitan los protocolos e interfaces establecidos en el anexo I para la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos a unidades de cartera.».

4) El artículo 5 se modifica como sigue:

   a) Los apartados 1 y 2 se sustituyen por el texto siguiente:

   «1. Los proveedores de carteras se asegurarán de que las soluciones de cartera admitan protocolos e interfaces para la presentación de atributos a las partes usuarias de la cartera, a distancia y, cuando proceda, en proximidad, de conformidad con las especificaciones técnicas establecidas en el anexo II.

   2. Los proveedores de carteras se asegurarán de que, a petición de los usuarios, las unidades de cartera respondan a las solicitudes autenticadas y validadas de las partes usuarias de la cartera a que se refiere el artículo 3, de conformidad con las especificaciones técnicas establecidas en el anexo II.».

   b) Se suprime el apartado 5.

5) El artículo 8 se sustituye por el texto siguiente:

«*Artículo 8*

Entrada en vigor

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

El artículo 3, apartado 4, será aplicable a partir del 11 de agosto de 2028.

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

6) Se suprime el anexo.

7) Se añade como anexo I el texto que figura en el anexo XI del presente Reglamento.

8) Se añade como anexo II el texto que figura en el anexo XII del presente Reglamento.

Artículo 5

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 15 de julio de 2026.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

«ANEXO

Especificaciones técnicas para los datos de identificación de la persona a que se refiere el artículo 3, apartado 3

1) Sección 1: Conjunto de datos de identificación de la persona física

Cuadro 1

Datos obligatorios de identificación de la persona correspondientes a la persona física para la divulgación selectiva

Identificador de los datos	Definición
`family_name`	Apellido actual o apellidos actuales del usuario al que se refieren los datos de identificación de la persona.
`given_name`	Nombre actual, incluidos los segundos nombres, en su caso, del usuario al que se refieren los datos de identificación de la persona.
`birth_date`	Día, mes y año en que nació el usuario al que se refieren los datos de identificación de la persona.
`birth_place`	País, como código de país alfa-2 especificado en la norma ISO 3166-1, o Estado, provincia, distrito o región, o municipio, ciudad o pueblo en que nació el usuario al que se refieren los datos de identificación de la persona.
`nationality`	Uno o varios códigos de país alfa-2 especificados en la norma ISO 3166-1, que representen la nacionalidad del usuario al que se refieren los datos de identificación de la persona.
`portrait`	Excepto cuando el usuario opte explícitamente por no incluir su retrato, cuando proceda, la imagen facial del usuario al que se refieren los datos de identificación de la persona que cumpla los requisitos de calidad para un tipo de imagen frontal completa establecidos en la norma ISO/IEC 39794-5, o, para la retrocompatibilidad, la norma ISO/IEC 19794-5, cláusulas 8.2, 8.3 y 8.4, proporcionada como datos de imagen codificados y sin las cabeceras o bloques especificados en la cláusula 5 de la norma ISO/IEC 19794-5, excepto los propios datos de la imagen (JPEG), que será de aplicación a partir del 11 de agosto de 2028.

— Los Estados miembros podrán disponer que el usuario tenga la opción de negarse a introducir el retrato en los datos de identificación de la persona.

— Los Estados miembros velarán por que la divulgación selectiva se aplique a cada identificador de datos, incluido el retrato.

— Cuando no se conozca la fecha de nacimiento de la persona física, los Estados miembros elegirán valores adecuados que cumplan las especificaciones establecidas en las secciones 4.1 o 4.2 (según proceda) del presente anexo.

— Cuando se desconozca la nacionalidad de la persona física, los Estados miembros utilizarán el valor “QU”.

— Cuando la persona física no posea una nacionalidad, los Estados miembros utilizarán el valor “QS”.

— Cuando el usuario opte por no incluir su retrato, los Estados miembros dejarán el valor vacío.

Cuadro 2

Datos opcionales de identificación de la persona correspondientes a la persona física para la divulgación selectiva

Identificador de los datos	Definición
resident_address	Dirección completa del lugar en el que reside actualmente el usuario al que se refieren los datos de identificación de la persona (nombre de la calle, número de la casa, ciudad, etc.) o en la que se le puede contactar.
resident_country	País en el que reside actualmente el usuario al que se refieren los datos de identificación de la persona, como código de país alfa-2 especificado en la norma ISO 3166-1.
resident_state	Estado, provincia, distrito o región en que reside actualmente el usuario al que se refieren los datos de identificación de la persona.
resident_city	Municipio, ciudad o pueblo en que reside actualmente el usuario al que se refieren los datos de identificación de la persona.
resident_postal_code	Código postal del lugar en el que reside actualmente el usuario al que se refieren los datos de identificación de la persona.
resident_street	El nombre de la calle en la que reside actualmente el usuario al que se refieren los datos de identificación de la persona, incluido el número de la casa y cualquier afijo o sufijo de este.
personal_administrative_-number	Un valor asignado al usuario al que se refieren los datos de identificación de la persona que sea único entre todos los números administrativos personales expedidos por el proveedor de datos de identificación de la persona. Cuando los Estados miembros opten por incluir este atributo, describirán, en sus sistemas de identificación electrónica en cuyo marco se expidan los datos de identificación de la persona, la política que aplican a los valores de este atributo, y en concreto, en su caso, las condiciones específicas para el tratamiento de este valor.
family_name_birth	Apellido o apellidos actuales del usuario al que se refieren los datos de identificación de la persona en el momento de su nacimiento.
given_name_birth	Nombre o nombres, incluidos los segundos nombres, del usuario al que se refieren los datos de identificación de la persona en el momento de su nacimiento.
sex	El valor será uno de los siguientes: 0 = desconocido; 1 = masculino; 2= femenino; 3 = otro; 4 = intersexual; 5 = diverso; 6 = no conforme; 9 = no procede; Para los valores 0, 1, 2 y 9, se aplica la norma ISO/IEC 5218.
email_address	Dirección de correo electrónico del usuario al que se refieren los datos de identificación de la persona [de conformidad con el estándar RFC 5322 ([1])].

Identificador de los datos	Definición
`mobile_phone_number`	Número de teléfono móvil del usuario al que se refieren los datos de identificación de la persona, empezando por el símbolo "+" como prefijo del código internacional y el código de país, seguido únicamente de números.

([1]) P. Resnick, Ed., "Internet Message Format," RFC 5322, octubre de 2008.

2) Sección 2: Conjunto de datos de identificación de la persona jurídica

Cuadro 3

Datos de identificación de la persona obligatorios para la persona jurídica

Identificador de los datos
razón social actual
identificador único construido por el Estado miembro remitente de conformidad con las especificaciones técnicas a efectos de identificación transfronteriza y que sea lo más perdurable posible

— Cuando un identificador de datos correspondiente a la persona no se conozca o no pueda expedirse de otro modo como parte del conjunto de datos que la identifican, los Estados miembros utilizarán en su lugar el valor de un atributo adecuado a la situación.

Cuadro 4

Datos de identificación de la persona opcionales para la persona jurídica

Identificador de los datos
dirección actual
número de identificación a efectos del IVA
número de identificación fiscal
identificador único europeo a que se refiere la Directiva (UE) 2017/1132 del Parlamento Europeo y del Consejo ([1])
identificación de entidad jurídica (LEI) a que se refiere el Reglamento de Ejecución (UE) 2022/1860 de la Comisión ([2])
número de registro e identificación de agente económico (EORI) a que se refiere el Reglamento de Ejecución (UE) n.º 1352/2013 de la Comisión ([3])
número de impuestos especiales establecido en el artículo 2, punto 12, del Reglamento (UE) n.º 389/2012 del Consejo ([4])

([1]) Directiva (UE) 2017/1132 del Parlamento Europeo y del Consejo, de 14 de junio de 2017, sobre determinados aspectos del Derecho de sociedades (DO L 169 de 30.6.2017, p. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/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 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).

([4]) 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).

3) Sección 3: Conjunto de metadatos sobre los datos de identificación de la persona

Cuadro 5

Metadatos sobre los datos de identificación de la persona

Identificador de los datos	Definición	Presencia
`issuing_authority`	Nombre de la autoridad administrativa que expidió los datos de identificación de la persona, o código de país alfa-2 ISO 3166 del Estado miembro correspondiente si no hay una autoridad independiente facultada para expedir datos de identificación de la persona.	obligatoria
`issuing_country`	Código de país alfa-2, según se especifica en la norma ISO 3166-1, del país o el territorio del proveedor de los datos de identificación de la persona.	obligatoria
`expiry_date`	Fecha (y, si es posible, hora) en que expirará el período de validez administrativa de los datos de identificación de la persona.	opcional
`document_number`	Número asignado a los datos de identificación de la persona por el proveedor de esos datos.	opcional
`issuing_jurisdiction`	Código de subdivisión de país de la jurisdicción que expidió los datos de identificación de la persona, según lo especificado en la norma ISO 3166-2:2020, cláusula 8. La primera parte del código coincidirá con el valor correspondiente al país expedidor.	opcional
`issuance_date`	Fecha (y, si es posible, hora) en que comenzó el período de validez administrativa de los datos de identificación de la persona.	opcional

4) Sección 4: Codificación de los atributos de los datos de identificación de la persona física

— Los datos de identificación de la persona física se expedirán de conformidad con las normas establecidas en el anexo II del Reglamento de Ejecución (UE) 2024/2979, cláusulas 5 (formato SD-JWT VC) y 6 (formato ISO/IEC-mdoc), aplicables a las declaraciones electrónicas de atributos. No se aplicarán las cláusulas 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3,6.2.4 y 6.2.5

— La codificación de los datos de identificación de la persona física deberá cumplir las especificaciones técnicas de las secciones 4.1 y 4.2 del presente anexo.

4.1 Codificación de los datos de identificación de la persona física en formato ISO/IEC-mdoc

— El tipo de declaración para los datos de identificación de la persona en formato ISO/IEC mdoc será “eu.europa.ec.eudi.pid.1”. El identificador del espacio de nombres para los atributos de los datos de identificación de la persona establecidos en el presente anexo será “eu.europa.ec.eudi.pid.1”.

— Cuando los datos de identificación de la persona incluyan datos cuyos identificadores de datos no figuren en el presente anexo, dichos datos se definirán en un espacio de nombres de datos de identificación de la persona nacional que utilice el formato general eu.europa.ec.eudi.pid. [código de país ISO 3166-1 alfa-2 o código de región ISO 3166-2] seguido de un punto opcional y un número de versión.

— Cuando se utilice el espacio de nombres nacional, su sistema, incluidos todos los identificadores de datos, sus definiciones, presencia y formatos de codificación, se publicará de conformidad con el artículo 8 del Reglamento de Ejecución (UE) 2025/1569 de la Comisión ([1]).

— Los datos de identificación de la persona y sus metadatos establecidos en las secciones 1 y 3 del presente anexo se incluirán en los elementos de datos de identificación de la persona en el sentido de las especificaciones de formato ISO/IEC mdoc.

— El miembro deviceKey perteneciente al miembro deviceKeyInfo de la instancia del tipo MobileSecurityObject contendrá una clave pública.

— Dicha clave pública corresponderá a una clave privada almacenada en el dispositivo criptográfico seguro de cartera (WSCD) del usuario de la cartera.

— La cabecera protegida de la firma digital CB-AdES que firme los datos de identificación de una persona en formato ISO/IEC-mdoc contendrá los parámetros de cabecera x5u y x5t, ambos especificados en RFC 9360 ([2]).

— El algoritmo de resumen utilizado en el parámetro de cabecera x5t será SHA-256.

— Los requisitos para codificar los datos de identificación de la persona en formato ISO/IEC-mdoc se establecen en el cuadro 6:

Cuadro 6

Requisitos para la codificación de los datos de identificación de la persona en formato ISO/IEC-mdoc

Identificador de los datos	Identificador del atributo	Formato de codificación
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Reglamento de Ejecución (UE) 2025/1569 de la Comisión, de 29 de julio de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las declaraciones electrónicas cualificadas de atributos y las declaraciones electrónicas de atributos proporcionadas por un organismo del sector público responsable de una fuente auténtica, o en nombre de este (DO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates" (https://datatracker.ietf.org/doc/rfc9360/).

Identificador de los datos	Identificador del atributo	Formato de codificación
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate o full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate o full-date

— La notación del formato de codificación de los atributos especificados en el cuadro 6 utilizará los tipos de representación especificados en RFC 8610 ([3]), con los siguientes requisitos adicionales:

a) un tstr se codificará en UTF-8;

b) un tstr soportará todo el rango Unicode;

c) un tstr tendrá una longitud máxima de 150 caracteres;

d) una fecha se codificará como se especifica en RFC 8943 ([4]);

e) una fecha completa se interpretará como #6.1004(tstr), donde tag 1004 es como se especifica en RFC 8943;

f) un atributo tdate contendrá una cadena de fecha-hora, según se especifica en RFC 3339 ([5]);

g) un atributo full-date contendrá una cadena de full-date, según se especifica en RFC 3339, de conformidad con RFC 8943;

h) salvo indicación en contrario, la representación de una fecha en atributos:

— no utilizará fracciones de segundos;

— no utilizará ninguna desviación local del tiempo universal coordinado (TUC) y la desviación del tiempo especificada en RFC 3339 se establecerá como "Z".

i) un número entero con los tipos mayores 0 y 1 deberá ser lo más pequeño posible, según se especifica en RFC 8949 ([6]), sección 4.2;

j) un place_of_birth contendrá al menos uno de los siguientes pares clave-valor: "country", "region" o "locality";

k) la expresión de la longitud en un bstr, tstr, *array* o mapa será lo más corta posible, según se especifica en RFC 8949, sección 4.2;

([3]) C. Vigano and H. Birkholz, "Concise Data Definition Language (CDDL): A Notational Convention to Resolve Ambiguities in JSON and CBOR Data Structures," RFC 8610, junio de 2019.
([4]) M. Jones, A. Nadalin and J. Richter, "Concise Binary Object Representation (CBOR) Tags for Date", RFC 8943, noviembre de 2020.
([5]) G. Klyne and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, julio de 2002.
([6]) C. Bormann and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 8949, diciembre de 2020.

l) el atributo de nacionalidad se codificará como un *array* de códigos de país alfa-2, según se especifica en ISO 3166-1. Cuando se utilice la notación CDDL según se especifica en RFC 8610, la codificación de este atributo será:

— nationalities = [+ CountryCode];

— CountryCode = tstr; código de país alfa-2 especificado en la norma ISO 3166-1;

— cuando un usuario de una cartera al que se refieran los datos de identificación de la persona tenga múltiples nacionalidades y el proveedor de datos de identificación de la persona las declare, el proveedor de datos de identificación de la persona podrá incluir todas las nacionalidades en los datos de identificación de la persona;

— el atributo place_of_birth se codificará como tipo place_of_birth. Cuando se utilice la notación CDDL según se especifica en RFC 8610, la codificación de este atributo será:

place_of_birth =

{

? "country": tstr; un único código de país alfa-2 según se especifica en la norma ISO 3166-1

? "region": tstr; el nombre de un estado, provincia, distrito o zona local

? "locality": tstr; el nombre de un municipio, ciudad o pueblo

}

4.2 Requisitos para la codificación de los datos de identificación de la persona en formato SD-JWT VC

— Los datos de identificación de la persona y sus metadatos especificados en la presente sección se incluirán en los datos de identificación de la persona como declaraciones en el sentido de las especificaciones de formato SD-JWT VC.

— Todas las declaraciones de los datos de identificación de la persona expedidos a que se refiere el guion anterior serán divulgables selectivamente de forma individual, excepto las declaraciones definidas como no divulgables de selectivamente en formato SD-JWT VC.

— El cuadro 7 especifica la codificación de los nombres de declaración que son nombres públicos.

— El cuadro 8 especifica la codificación de los nombres de declaración que son específicos de los datos de identificación de la persona.

— Una cadena JSON utilizada en los datos de identificación de la persona codificados en SD-JWT VC se codificará en UTF-8 y soportará todo el rango Unicode, a menos que se especifique expresamente lo contrario en el cuadro 8 que figura a continuación o en las referencias que figuran en él.

— Las declaraciones JWT nbf y exp, tal como se definen en RFC 7519 ([7]), se utilizarán para expresar el período de validez técnica de los datos de identificación de la persona conformes con el formato SD-JWT VC.

([7]) J. Jones, *et al.*, "JSON Web Token (JWT)", RFC 7519, mayo de 2015.

— Los datos de identificación de la persona incorporarán la declaración cnf, tal como se define en la RFC 7800 ([8]), que será una clave pública generada a partir de una clave privada almacenada en el WSCD de la unidad de cartera del usuario de la cartera.

— La cabecera protegida de la firma digital que firme los datos de identificación de una persona en formato SD-JWT VC contendrá los parámetros de cabecera x5u y x5t#S256, según se especifican en RFC 7515 ([9]).

Cuadro 7

Requisitos para la codificación de los datos de identificación de la persona en formato SD-JWT VC utilizando nombres públicos

Identificador de los datos	Identificador del atributo	Formato de codificación
`family_name`	`family_name`	cadena
`given_name`	`given_name`	cadena
`birth_date`	`birthdate`	cadena, ISO 8601-1, formato YYYY-MM-DD
`birth_place`	`place_of_birth`	estructura JSON
`nationality`	`nationalities`	*array* de cadenas
`resident_address`	`address.formatted`	cadena
`resident_country`	`address.country`	cadena
`resident_state`	`address.region`	cadena
`resident_city`	`address.locality`	cadena
`resident_postal_code`	`address.postal_code`	cadena
`resident_street`	`address.street_address`	cadena
`family_name_birth`	`birth_family_name`	cadena
`given_name_birth`	`birth_given_name`	cadena
`email_address`	`email`	cadena
`mobile_phone_number`	`phone_number`	cadena
`portrait`	`picture`	cadena; URL de los datos que contiene un retrato codificado en base64 en formato JPEG

([8]) M. Jones, *et al.*, "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)", RFC 7800, abril de 2016.
([9]) M. Jones, *et al.*, "JSON Web Signature (JWS)", RFC 7515, mayo de 2015.

Cuadro 8

Requisitos para la codificación de los datos de identificación de la persona en formato SD-JWT VC utilizando nombres privados

Identificador de los datos	Identificador del atributo	Formato de codificación
`expiry_date`	`date_of_expiry`	cadena, ISO 8601-1, formato YYYY-MM-DD
`issuance_date`	`date_of_issuance`	cadena, ISO 8601-1, formato YYYY-MM-DD
`personal_administrative_number`	`personal_administrative_number`	cadena
`sex`	`sex`	número
`issuing_authority`	`issuing_authority`	cadena
`issuing_country`	`issuing_country`	cadena
`document_number`	`document_number`	cadena
`issuing_jurisdiction`	`issuing_jurisdiction`	cadena

— El tipo básico de datos de identificación de la persona será "urn:eudi:pid:1", incluido en la declaración vct. Todos los datos de identificación de la persona utilizarán tipos en el espacio de nombres "urn:eudi:pid:".

— Cuando los datos de identificación de la persona incluyan atributos que no estén especificados en el presente anexo, estos se definirán dentro de un tipo nacional.

— Cuando se utilice el tipo nacional, su sistema, incluidos todos los identificadores de datos, sus definiciones y formatos de presencia y codificación, se establecerá en un sistema que se publique de conformidad con el artículo 8 del Reglamento de Ejecución (UE) 2025/1569.

5) Sección 5: Detalles de la infraestructura de confianza

La lista de proveedores de datos de identificación de la persona facilitada por la Comisión de conformidad con el Reglamento de Ejecución (UE) 2024/2980 permitirá la autenticación de los datos de identificación de la persona.».

ANEXO II

«*ANEXO I bis*

Mecanismos criptográficos a que se refiere el artículo 5 *bis*

Grupo Europeo de Certificación de la Ciberseguridad, Subgrupo de Criptografía: "Agreed Cryptographic Mechanisms", publicado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) [1].».

[1] https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

ANEXO III

«*ANEXO I ter*

Especificaciones técnicas para las declaraciones de unidad de cartera a que se refiere el artículo 6, apartado 2 *bis*

1) Una declaración de unidad de cartera comprenderá una o varias declaraciones de instancia de cartera y una o varias atestaciones de clave.

2) La declaración de instancia de cartera y las atestaciones de clave cumplirán los siguientes requisitos:

a) Requisitos de formato

— FR-WIA-1: Una declaración de instancia de cartera será un JSON Web Token (JWT), según se especifica en RFC 7519 ([1]), que ha sido objeto de firma o de sellado por el proveedor de la cartera mediante una firma JAdES básica B de carácter compacto.

— FR-WIA-1.1: Una declaración de instancia de cartera será una declaración de cartera según se especifica en el apéndice E de "OpenID for Verifiable Credential Issuance v1.0" ([2]) (OID4VCI) y ampliada como se especifica más adelante en C-WIA-1 y C-WIA-2.

— FR-KA-1: Una atestación de clave será un JWT, según se especifica en RFC 7519, que ha sido objeto de firma o de sellado por el proveedor de la cartera mediante una firma JAdES básica B de carácter compacto.

— FR_KA_1.1: Una atestación de clave será una atestación de clave según lo especificado en el apéndice D de OID4VCI, ampliada según lo especificado más adelante en C_KA-1 y C_KA-2.

b) Requisitos de transporte

— TR-WIA-1: Una unidad de cartera utilizará una declaración de instancia de cartera durante la expedición de datos de identificación de la persona, declaraciones electrónicas cualificadas o no cualificadas de atributos o declaraciones electrónicas de atributos facilitadas por un organismo del sector público responsable de una fuente auténtica o en nombre de este.

— TR-WIA-2: Los proveedores de carteras verificarán la integridad de la instancia de cartera y firmarán o sellarán la declaración de instancia de cartera.

— TR-WIA-2.1: Cuando un proveedor de cartera expida una declaración de instancia de cartera, la diferencia entre la hora en que el proveedor de cartera verificó la integridad de la instancia de cartera y la hora que indicará en el parámetro de cabecera "exp" de la declaración de instancia de cartera expedida será inferior a 24 horas.

— TR-WIA-2.2: El proveedor de cartera se asegurará de que una unidad de cartera contenga las declaraciones de instancia de cartera necesarias para la expedición de datos de identificación de la persona y las declaraciones electrónicas de atributos.

— TR-WIA-3: Durante la emisión, una unidad de cartera enviará una declaración de instancia de cartera al servidor de autorización en la petición de autorización impulsada (*pushed*) y la petición de token, según se especifica en OID4VCI.

— TR-WIA-3.1: Una unidad de cartera enviará la declaración de instancia de cartera junto con una prueba de posesión (PoP), según se especifica en el apéndice E de OID4VCI.

— TR-WIA-3.2: Una unidad de cartera enviará la misma declaración de instancia de cartera a solamente un servidor de autorización.

([1]) RFC 7519: JSON Web Token (JWT), mayo de 2015.
([2]) OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Cuando un proveedor de cartera utilice la opción de "per-issuer reuse" especificada en R_WIA_1, una unidad de cartera podrá enviar una declaración de instancia de cartera al mismo servidor de autorización varias veces.

— TR-WIA-3.2.2: Cuando un proveedor de cartera no utilice la opción de "per-issuer reuse", una unidad de cartera utilizará una declaración de instancia de cartera como máximo en un proceso de expedición.

— TR-WIA-4: Cuando un servidor de autorización reciba una declaración de instancia de cartera, verificará la firma de la declaración de instancia de cartera utilizando la clave pública del certificado de firma incluido en el parámetro “x5c” de la cabecera JOSE de la declaración de instancia de cartera.

— TR-WIA-4.1: El servidor de autorización también verificará que este certificado de firma pueda verificarse con un ancla de confianza en la lista de proveedores de carteras a que se refiere el artículo 5 del Reglamento de Ejecución (UE) 2024/2980, posiblemente utilizando certificados intermedios incluidos en el parámetro x5c.

— TR-WIA-4.2: El servidor de autorización verificará que la declaración de instancia de cartera no ha expirado.

— TR-WIA-4.3: El servidor de autorización verificará la firma del punto de entrada bajo la clave pública presente en la declaración “cnf”.

— TR_KA-1: Una unidad de cartera utilizará una atestación de clave durante la expedición de los datos de identificación de la persona y durante la expedición de declaraciones electrónicas cualificadas o no cualificadas de atributos vinculadas a un producto, o declaraciones electrónicas de atributos facilitadas por un organismo del sector público responsable de una fuente auténtica o en nombre de este.

— TR_KA-1.1: Una unidad de cartera no utilizará una atestación de clave durante la expedición de declaraciones electrónicas cualificadas o no cualificadas de atributos no vinculadas a un producto, o declaraciones electrónicas de atributos proporcionadas por un organismo del sector público responsable de una fuente auténtica o en nombre de este.

— TR_KA-2: Un proveedor de cartera proporcionará una unidad de cartera con diferentes atestaciones de clave para el WSCD de la unidad de cartera y para cada uno de sus almacenes de claves.

— TR_KA-2.1: El proveedor de cartera firmará o sellará una atestación de clave, después de que haya verificado que las claves declaradas en la atestación de clave estén almacenadas en el WSCD de la unidad de cartera o almacén de claves descrito en la atestación de clave.

— TR_KA-2.2: Una atestación de clave contendrá como mínimo una clave pública declarada. El número de claves de la atestación de clave enviada a un expedidor de credenciales no superará el tamaño máximo de lote especificado por dicho expedidor de credenciales en sus metadatos del expedidor de credenciales; véase ETSI TS 119 472-3 ([3]), parámetro “credential_configurations_supported.” credential_metadata.credential_reuse_policy.options.batch_size.

— TR_KA-2.3: Un proveedor de cartera incluirá una clave pública (correspondiente a una clave privada almacenada en el WSCD o en el almacén de claves de la unidad de cartera) en como máximo una sola atestación de clave.

— TR_KA-2.4: Una unidad de cartera utilizará una atestación de clave durante, como máximo, un proceso de expedición o reexpedición de credenciales.

— TR_KA-2.5: El proveedor de una cartera se asegurará de que una unidad de cartera esté en posesión de las atestaciones de clave necesarias para la expedición de los datos de identificación de la persona y las declaraciones electrónicas de atributos vinculadas a un dispositivo.

([3]) ETSI, “Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles”, ETSI TS 119 472-3, V1.1.1, marzo de 2026.

— TR_KA-3: Cuando sea necesario durante la expedición, una unidad de cartera incluirá una atestación de clave en el campo “proofs” de una petición de credencial al expedidor de la credencial, según se especifica en OID4VCI, en una prueba de tipo “jwt” o de tipo “attestation”.

— TR_KA_3.1: Cuando una unidad de cartera incluya una atestación de clave en un elemento “jwt”, firmará o sellará la atestación de clave utilizando la clave privada correspondiente a la clave pública al índice 0 del *array* “attested_keys” del objeto “key_attestation”.

— TR_KA-4: Cuando un expedidor de credenciales expida credenciales vinculadas a un dispositivo, indicará en el parámetro “proof_types_supported” de sus metadatos de credenciales de expedidor, según se especifica en la sección 12.2.4 de OID4VCI, que soporta tanto el tipo de prueba “jwt” como el de “attestation” para las atestaciones de clave que incluirán el objeto “key_attestation_required”.

— TR_KA-4.1: Cuando un expedidor de credenciales expida credenciales no vinculadas a un producto, omitirá los parámetros “proof_types_supported” y “cryptographic_binding_methods_-supported” en los metadatos del expedidor de credenciales.

— TR_KA-5: Cuando un expedidor de credenciales reciba una atestación de clave en un tipo de prueba “jwt” o “attestation”, verificará la firma de la atestación de clave de la clave pública del certificado de firma incluido en el parámetro “x5c” en la cabecera JOSE de la atestación de clave y que este certificado de firma con un ancla de confianza esté en la lista de proveedores de carteras a que se refiere el artículo 5 del Reglamento de Ejecución (UE) 2024/2980, posiblemente utilizando certificados intermedios incluidos en el parámetro “x5c”.

— TR_KA-6: Cuando un expedidor de credenciales reciba una atestación de clave en un tipo de prueba “jwt”, verificará la firma del elemento “jwt” de la clave del índice 0 del conjunto del *array* “attested_keys” del objeto “key_attestation” incluido en el elemento “jwt”.

— TR_KA-6.1: El expedidor de la credencial verificará que el campo “nonce” del elemento “jwt” incluye un “c_nonce” válido de su “nonce_endpoint”, como se especifica en OID4VCI.

— TR_KA-7: Cuando un expedidor de credenciales reciba una atestación de clave en un tipo de prueba “attestation”, verificará que el objeto “key_attestation” incluye un “c_nonce” válido de su “nonce_endpoint”.

— TR_KA-8: El proveedor de datos de identificación de la persona se asegurará de que los datos de identificación de la persona estén vinculados a una clave pública que tenga su origen en una atestación de clave que mencione un WSCD.

c) Requisitos de contenido

— C_WIA-1: Una declaración de instancia de cartera incluirá lo siguiente:

— la declaración “wallet_name” especificada en el apéndice E de OID4VCI, cuyo valor será el identificador de la solución de cartera que puede encontrarse en la lista de proveedores de carteras a que se refiere el artículo 5 del Reglamento de Ejecución (UE) 2024/2980;

— una declaración de “wallet_version” ([4]), que será una cadena cuyo valor será la versión de la solución de cartera;

— una declaración de “wallet_solution_certification_information”, que será un objeto JSON que contiene información sobre el organismo de evaluación de la conformidad que certificó la solución de cartera, el número de certificación, según proceda, y otros detalles pertinentes en lo que respecta a la certificación;

([4]) Esta declaración se define en el presente Reglamento de Ejecución de la Comisión, ya que no forma parte de la especificación OID4VCI.

— una declaración de “client_status”, que contiene dos subcampos:

  — “status”: una referencia a la lista de estados según se especifica en el apéndice E de OID4VCI que representa el estado de revocación de la instancia de cartera. Para más información, véase la sección e) siguiente;

  — “exp”: una “NumericDate”, según se especifica en el RFC 7519, que establece el tiempo hasta el cual el proveedor de la cartera mantendrá el estado de revocación en el índice de la lista de estados al que se hace referencia en “status”;

— la declaración “exp” especificada en el apéndice E de OID4VCI.

— *NOTA*: La declaración “client_status.status” en una declaración de instancia de cartera representa el estado de revocación de la instancia de cartera, no el estado de revocación de la declaración misma. Como se describe en R_WIA-1 más adelante, un proveedor de cartera puede decidir limitar el ámbito de cada declaración de instancia de cartera a un servidor de autorización específico sobre la base del hecho de que todas las declaraciones enviadas a dicho servidor contienen el mismo valor de índice en la entrada “client_status.status”.

— *NOTA*: El valor “idx” de la declaración de “status” puede utilizarse como identificador único (de pares) de la instancia de cartera y de la unidad de cartera.

— C_WIA-2: Una declaración de instancia de cartera también debe incluir la declaración “wallet_link” especificada en el apéndice E de OID4VCI y el valor de esta declaración será un URI en el que pueda obtenerse más información sobre la solución de cartera.

— C_WIA-3: Un servidor de autorización no interpretará el parámetro “exp” en el nivel superior de una declaración de instancia de cartera como el final del período de mantenimiento de revocación de la instancia de cartera.

— *NOTA*: El parámetro “exp” en el nivel superior de una declaración de instancia de cartera indica cuándo expira la declaración misma.

— C_KA-1: Una atestación de clave incluirá:

  — las declaraciones “key_storage” y “user_authentication” especificadas en el apéndice D de OID4VCI;

    — los atributos “key_storage” y “user_authentication” tendrán valor “iso_18045_high” cuando una atestación de clave mencione un WSCD;

  — la declaración “certification” especificada en el apéndice D de OID4VCI, que contiene un URL en el que puede obtenerse información sobre la certificación obtenida por el WSCD o el almacén de claves, a título indicativo el sistema, como Common Criteria o GlobalPlatform, los requisitos evaluados, como el perfil de protección aplicable, y el nivel de evaluación;

    — a partir de esta información será posible determinar si la clave está almacenada en un WSCD;

  — una declaración de “key_storage_status”, que contiene dos subcampos:

    — “status”: una referencia a una lista de estados según se especifica en el apéndice D.1 de OID4VCI. El valor representa, bien el estado de revocación del WSCD, bien el tipo de almacén de claves utilizado para almacenar las claves declaradas, bien, con la opción de índice “per-key-attestation”, el estado de revocación del WSCD o del almacén de claves de una unidad de cartera concreta. Véase R_KA_1 más adelante para consultar las opciones de asignación de índices disponibles;

    — “exp”: una “NumericDate”, según se especifica en el RFC 7519, que establece el tiempo hasta el cual el proveedor de la cartera mantendrá el estado de revocación en el índice de la lista de estados al que se hace referencia en “status”;

  — la declaración “exp” especificada en el apéndice D de OID4VCI.

— *NOTA* sobre el valor de “idx” en la declaración “key_storage_status.status” de una atestación de clave: Cuando el proveedor de cartera emplee la opción “type-shared index” (véase R_KA_1 más adelante), todas las atestaciones de clave del mismo tipo de WSCD o de almacén de claves comparten el mismo índice de lista de estados. Por lo tanto, el valor “idx” no es único por unidad de cartera. Por el contrario, cuando el proveedor de la cartera utilice la opción “per-key-attestation index”, el valor de “idx” es único para la unidad de cartera (o único, de pares, por expedidor de credenciales). Sin embargo, en todos los casos, un expedidor de credenciales no utilizará el valor “idx” en una atestación de clave como identificador de unidad de cartera, sino que utilizará el valor “idx” en una declaración de instancia de cartera.

— C_KA-2: Cuando se envíe una atestación de clave en un tipo de prueba “attestation”, también incluirá un “c_nonce” válido, según se especifica en el apéndice F.3 de OID4VCI.

— C_KA-3: Un expedidor de una credencial no interpretará el parámetro “exp” en el nivel superior de una atestación de clave como el final del período de mantenimiento de revocación del WSCD o del almacén de claves.

— *NOTA*: El parámetro “exp” en el nivel superior de una atestación de clave indica cuándo expira la atestación de clave misma.

d) Requisitos del ciclo de vida

— El presente anexo especifica los siguientes parámetros de metadatos del expedidor de credenciales:

— “preferred_client_status_period”: OPTIONAL. Un número entero que especifique el período de mantenimiento del estado restante preferido de la declaración de instancia de cartera que debe presentar la unidad de cartera durante la expedición, expresado en segundos. El período de mantenimiento del estado restante se define como el valor de “client_status.exp” en la declaración menos el momento de recepción de la misma.

— “preferred_key_storage_status_period”: OPTIONAL. Un número entero que especifique el período de mantenimiento del estado restante preferido de la atestación de clave que debe presentar la unidad de cartera durante la emisión, expresado en segundos. El período de mantenimiento del estado restante se define como el valor “key_storage_status.exp” en la declaración menos el momento de recepción de la misma.

— LC_WIA-1: Un servidor de autorización puede comunicar sus preferencias para el período de mantenimiento del estado restante en las declaraciones de instancia de cartera mediante la inclusión del parámetro de metadatos “preferred_client_status_period” en su punto de conexión (*endpoint*) de metadatos del expedidor de la credencial, según se especifica en la sección 12.2.2 de OID4VCI.

— LC_WIA-1.1: Este campo se situará en el nivel superior de los metadatos del expedidor de la credencial.

— LC_WIA_2: Un servidor de autorización no interpretará el parámetro “exp” en el nivel superior de una declaración de instancia de cartera como el final del período de mantenimiento de revocación de la instancia de cartera.

— LC_WIA_3: Cuando un proveedor de cartera firme o selle una declaración de instancia de cartera, mantendrá el estado de revocación de la instancia de cartera pertinente hasta que haya superado la “wallet_instance_status.exp” indicada en dicha declaración de instancia de cartera.

— LC_KA-1: Cuando sea necesaria una atestación de clave, el expedidor de una credencial podrá comunicar sus preferencias para el período de mantenimiento del estado restante en las atestaciones de clave mediante la inclusión del parámetro de metadatos “preferred_key_storage_status_period” especificado anteriormente en su punto de conexión de metadatos del expedidor de credenciales, según se especifica en la sección 12.2.2 de OID4VCI.

— LC_KA-1.1: Este campo se situará dentro del objeto “key_attestations_required”, según se especifica en la sección 12.2.4 de OID4VCI.

— LC_KA-2: El proveedor de una cartera elegirá el período de validez técnica de las atestaciones de clave que expida.

— LC_KA-3: Cuando un proveedor de cartera firme o selle una atestación de clave, mantendrá el estado de revocación del WSCD o del almacén de claves pertinente hasta que haya superado la "key_storage_status.exp" indicada en dicha atestación de clave.

— LC_GEN-1: Un proveedor de cartera se asegurará de que una unidad de cartera pueda presentar siempre declaraciones de unidad de cartera y atestaciones de clave cuyos "client_status.exp" y "key_storage_status.exp" (respectivamente) se sitúen al menos 31 días en el futuro en el momento de su presentación a un servidor de autorización o a un expedidor de credenciales.

— *NOTA*: Esto garantiza que los proveedores de datos de identificación de la persona puedan confiar en el encadenamiento de revocaciones sin verse obligados a expedir datos de identificación de la persona de corta duración.

— LC_GEN-2: Un proveedor de carteras se asegurará de que una unidad de cartera reciba los metadatos del expedidor de credenciales durante la expedición.

  — LC_GEN_2.1: Si se incluye un campo "preferred_key_storage_status_period" en estos metadatos, la unidad de cartera enviará una atestación de clave con ("key_storage_status.exp" − hora actual) − "preferred_key_storage_status_period" lo más pequeña posible, pero no negativa. Si la unidad de cartera no dispone de dicha atestación de clave, obtendrá una nueva atestación de clave del proveedor de la cartera que satisfaga el criterio "key_storage_status.exp" − hora actual ≥ "preferred_key_storage_status_period".

  — LC_GEN_2.2: Si se incluye un campo "preferred_client_status_period" en estos metadatos, la unidad de cartera enviará una declaración de instancia de cartera con ("client_status.exp" − hora actual) − "preferred_client_status_period" lo más pequeña posible, pero no negativa. Si la unidad de cartera no dispone de dicha declaración de instancia de cartera, solicitará una nueva declaración de instancia de cartera al proveedor de la cartera que satisfaga el criterio "client_status.exp" − hora actual ≥ "preferred_client_status_period".

— LC_GEN-3: El período de validez técnica de los datos de identificación de la persona finalizará antes tanto del "client_status.exp" de la declaración de instancia de cartera como del "key_storage_status.exp" de la atestación de clave enviada al proveedor de datos de identificación de la persona en el proceso de expedición.

— LC_GEN-4: Un proveedor de datos de identificación de la persona que tenga un período de validez técnica de más de 24 horas comprobará el estado de revocación tanto de la declaración de instancia de cartera como de la atestación de clave recibidas durante la expedición al menos una vez cada 24 horas durante el período de validez técnica de los datos de identificación de la persona. En caso de que se revoque cualquiera de ellos, el proveedor revocará los datos de identificación de la persona.

e) Requisitos de revocación

— R_GEN-1: Los proveedores de carteras utilizarán las listas de estados de los *token* (especificadas en la lista de estados de los *token* de IETF) como mecanismo de revocación tanto para las atestaciones de clave como para las declaraciones de instancia de cartera, según se especifica en los apéndices D y E de OID4VCI, respectivamente.

— *NOTA*: Para mejorar la escalabilidad de sus listas de estados, un proveedor de cartera puede utilizar las siguientes optimizaciones:

  — Dividir la lista de estados en múltiples bloques, cuando los proveedores de carteras tengan un número considerable de usuarios y hayan expedido declaraciones. Existen muchas estrategias para la elaboración de bloques, por ejemplo, basándose en un tamaño fijo o por períodos de tiempo. La estrategia de elaboración de bloques se deja a la discreción de los proveedores de carteras. Los factores pueden incluir el tamaño de una lista de estados para la descarga y la privacidad del usuario.

  — Tener múltiples listas de estados.

  — Comprimir una lista de estados para reducir su tamaño.

— R_WIA-1: Un proveedor de cartera puede asignar el mismo valor a la declaración “idx” en la declaración “client_status.status” en todas las declaraciones de instancia de cartera que una unidad de cartera determinada presente al mismo servidor de autorización. Esta opción se denomina “per-issuer reuse”. Si se utiliza esta opción:

  — R_WIA-1.1: La unidad de cartera mantendrá el estado en el que ha utilizado el valor del índice para cada servidor de autorización con el que haya interactuado previamente, y solicitará una declaración de instancia de cartera que contenga ese mismo valor del índice cuando vuelva a interactuar con el mismo servidor de autorización.

  — R_WIA-1.2: Cuando un proveedor de cartera reciba una petición de declaración de instancia de cartera que contenga un valor de índice específico, verificará que la unidad de cartera solicitante haya recibido previamente dicho valor de índice, antes de emitir una nueva declaración de instancia de cartera con dicho valor de índice.

  — R_WIA-1.3: La unidad de cartera no reutilizará el mismo valor de índice para interacciones con diferentes servidores de autorización.

— *NOTA*: Si se utiliza la opción de “per-issuer reuse”, el proveedor de cartera podrá determinar con cuántos servidores de autorización ha interactuado una unidad de cartera y con qué frecuencia interactúa con cada uno de ellos.

— R_WIA-2: En su política de privacidad, el proveedor de una cartera documentará si utiliza la opción de “per-issuer reuse” para la revocación de instancias de cartera.

— R_WIA-3: Cuando un proveedor de cartera no utilice la opción de “per-issuer reuse”, el proveedor de cartera asignará un valor de índice nuevo y no vinculable a cada declaración de instancia de cartera que expida.

— R_WIA-4: Cuando deba revocarse una unidad de cartera, el proveedor de cartera revocará los valores de índice de la declaración “client_status.status” en todas las declaraciones de instancia de cartera asociadas a dicha unidad de cartera.

— R_WIA-5: Un proveedor de cartera tendrán en cuenta la escala de su despliegue y la arquitectura subyacente a la hora de determinar el tamaño de sus listas de estados de declaraciones de instancia de cartera, garantizando que sean lo suficientemente grandes como para evitar las correlaciones y proteger la privacidad de los usuarios. Como mínimo, una lista de estados se referirá, en la medida de lo posible, a al menos 10 000 declaraciones.

— R_KA_1: Un proveedor de una cartera elegirá una de las siguientes opciones de asignación de índices para la declaración “key_storage_status.status” en una atestación de clave:

  — opción 1, denominada “type-shared index”, en la que todas las atestaciones de clave que declaran claves almacenadas en el mismo tipo de WSCD o almacén de claves contienen el mismo valor de índice en “key_storage_status.status”;

  — opción 2, denominada “per-key-attestion index”, en la que una atestación de clave que declare las claves almacenadas en un WSCD o en un almacén de claves concreto contiene un valor de índice único (de pares) en “key_storage_status.status”.

— *NOTA*: Cuando un proveedor de cartera utiliza la opción 1, una única acción de revocación invalida todas las atestaciones de clave del tipo afectado en todas las unidades de cartera. Además, dado que todas las atestaciones de clave para el mismo tipo de WSCD o almacén de claves comparten un único índice de la lista de estados, el número de entradas en una lista de estados de atestación de clave refleja el número de tipos de WSCD o de almacén de claves soportados por el proveedor de cartera, no el número de unidades de cartera desplegadas. Por lo tanto, las consideraciones de privacidad que motivan el tamaño mínimo de la lista de estados de las listas de estados de las instancias de cartera no se aplican a las listas de estados de las atestaciones de clave de la opción 1, siempre que haya suficientes unidades de cartera que utilicen el mismo tipo de dispositivo criptográfico o almacén de claves seguros de cartera.

— *NOTA*: Cuando un proveedor de cartera utilice la opción 2, cada índice representa el estado de revocación del WSCD o del almacén de claves específicos declarados en dicha atestación de clave.

— *NOTA*: Cuando un proveedor de cartera utilice la opción 2, también podrá revocarse, a petición del usuario, un WSCD o un almacén de claves específicos.

— R_KA-2: Cuando un proveedor de cartera utilice la opción 2, podrá utilizar opcionalmente la opción de "per-issuer reuse" descrita en R_WIA-1. Si el proveedor de la cartera utiliza esta opción, se aplicarán *mutatis mutandis* los requisitos R_WIA-1 — R_WIA-3.

— R_KA-3: Cuando un proveedor de cartera utilice la opción 2, tendrá en cuenta la escala de su despliegue y la arquitectura subyacente a la hora de determinar el tamaño de sus listas de estados de atestación de clave, garantizando que sean lo suficientemente grandes como para evitar la correlación y proteger la privacidad de los usuarios. Como mínimo, una lista de estados se referirá, en la medida de lo posible, a un mínimo de 10 000 atestaciones de clave.

— R_KA-4: Cuando un proveedor de cartera utilice la opción 1 ("type-shared index"), el proveedor de cartera solo revocará una entrada "key_storage_status.status" si el tipo de WSCD o de almacén de claves presenta una vulnerabilidad de seguridad.

f) Requisitos relativos a los algoritmos de firma

— SA-1: Para firmar declaraciones de instancia de cartera, atestaciones de clave, pruebas de posesión relacionadas y listas de estados de las fichas, se utilizará uno de los algoritmos siguientes:

— ES256 (ECDSA con SHA-256 y P-256)

— ES384 (ECDSA con SHA-384 y P-384)

— ES512 (ECDSA con SHA-512 y P-521)

— SA-2: Un proveedor de una cartera elegirá cuál de los algoritmos mencionados en SA-1 utilizará.

— SA-3: Un servidor de autorización o un expedidor de credenciales (según se especifica en OID4VCI) deberá soportar todos los algoritmos mencionados en SA-1.».

ANEXO IV

«*ANEXO II*

Lista de normas a que se refiere el artículo 8

Se aplican las especificaciones técnicas establecidas en las cláusulas 2 a 6 de ETSI TS 119 472-1 V1.2.1 (2026-02). Se leerán con las siguientes adaptaciones:

1) 2.1 Referencias normativas

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers".

— [25] IETF Token Status List (TSL), draft-ietf-oauth-status-list-20: "Token Status List", 20 de abril de 2026.

2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: Cuando se utilice un elemento de estado para los datos de identificación de la persona, las declaraciones electrónicas cualificadas de atributos o las declaraciones electrónicas de atributos facilitadas por un organismo del sector público responsable de una fuente auténtica o en nombre de este, solo indicará si la declaración está revocada o no y no soportará otros valores de estado, como la suspensión.

— EAA-4.2.11.1-06.1: Cuando una declaración esté revocada, estará revocada permanentemente.

3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: Cuando se expidan declaraciones electrónicas de atributos de corta duración con un período de validez de 24 horas o menos, no será necesaria la revocación.

4) 4.6.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)

— PuB-EAA-4.6.2-03: sin efecto.

— Pub-EAA-4.6.2-04: sin efecto.

— PuB-EAA-4.6.3-03: La firma digital de la PuB-EAA debe contener el certificado cualificado que admite la firma digital de la PuB-EAA.

— PuB-EAA-4.6.3-04: El certificado cualificado que admite la firma digital de la PuB-EAA cumplirá los requisitos de la cláusula 8 de ETSI TS 119 412-6 v1.1.1 e incluirá la QcType QcStatement según se define en ETSI EN 319 412-5 v2.5.1, con el valor id-etsi-qct-eidaspsbeaa definido como sigue:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Certificado contemplado en el art. 45 *septies*, apartado 1, letra b), que admite la firma electrónica cualificada o el sello electrónico cualificado del organismo del sector público a que se refiere el artículo 3, punto 46, del Reglamento (UE) n.º 910/2014.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: sin efecto.

— EAA-5.2.10.1-05: sin efecto.

— EAA-5.2.10.1-06: El miembro estado (*status*) podrá contener el miembro status_list según se especifica en la cláusula 6.2 de draft-ietf-oauth-status-list-20 de IETF [25].

— EAA-5.2.10.1-07: sin efecto.

— EAA-5.2.10.1-08: sin efecto.

— EAA-5.2.10.1-09: sin efecto.

— EAA-5.2.10.1-10: sin efecto.

— EAA-5.2.10.1-11: sin efecto.

— EAA-5.2.10.1-12: sin efecto.

6) 6.2.10.1 General requirements

— EAA-6.2.10.1-01: Cuando una declaración electrónica de atributos conforme con ISO/IEC mdoc utilice el mecanismo de lista de estados de la declaración establecido en EAA-6.2.10.1-02.2 o el mecanismo de lista de revocación de la declaración establecido en EAA-6.2.10.1-02.3, su objeto de seguridad móvil (Mobile Security Object, MSO) contendrá la estructura de estado, según se especifica en EAA-6.2.10.1-17, que contiene información sobre la revocación del MSO.

— EAA-6.2.10.1-01.1: Al implementar el mecanismo de lista de identificadores, el elemento de estado contendrá el elemento identifier_list según lo establecido en EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: Al implementar el mecanismo de lista de estados, el elemento de estado contendrá el elemento status_list según lo establecido en EAA-6.2.10.1-13.

— *NOTA*:

  — La estructura de estado contiene una referencia a una lista de revocación del MSO.

  — La lista de revocación del MSO es una estructura COSE_Sign1 que indica si un MSO concreto está revocado o no.

  — La estructura de estado contiene toda la información necesaria para que la parte usuaria de la cartera determine si la lista de revocación del MSO es auténtica.

— EAA-6.2.10.1-02: El proveedor de datos de identificación de la persona, el proveedor de declaraciones electrónicas cualificadas de atributos o el proveedor de declaraciones electrónicas de atributos facilitadas por un organismo del sector público responsable de una fuente auténtica o en nombre de este utilizarán uno de los siguientes métodos para la revocación de los datos de identificación de la persona, las declaraciones electrónicas cualificadas de atributos o las declaraciones electrónicas de atributos facilitadas por un organismo del sector público responsable de una fuente auténtica o en nombre de este:

— EAA-6.2.10.1-02.1: Cuando expidan declaraciones electrónicas de atributos de corta duración con un período de validez de 24 horas o menos, no se exigirá la revocación.

— EAA-6.2.10.1-02.2: Utilizarán un mecanismo de lista de estados de declaración para codificar la información sobre revocación como lista de estados.

— EAA-6.2.10.1-02.2.1: El mecanismo de lista de estados revoca un MSO en función de si el bit de la posición de bit definida por el expedidor en el MSO está establecida como verdadero en la lista de estados.

— EAA-6.2.10.1-02.2.2: El mecanismo de la lista de estados se especifica en la especificación de la lista de estados de *token* (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: Utilizarán un mecanismo de lista de revocaciones de declaración para codificar la información sobre revocación como lista de identificadores.

— EAA-6.2.10.1-02.3.1: El mecanismo de lista de identificadores revoca un MSO en función de si el identificador definido por el expedidor en el MSO está presente en la lista de identificadores.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 y EAA-6.2.10.1-11 especifican el mecanismo de lista de identificadores, sobre la base de los requisitos de la especificación de lista de estados de *token*, incluidas las características comunes a la lista de estatus y el mecanismo de lista de identificadores.

— EAA-6.2.10.1-03: Cuando un elemento de estado se utilice para datos de identificación de la persona, declaraciones electrónicas cualificadas de atributos o declaraciones electrónicas de atributos facilitadas por un organismo del sector público responsable de una fuente auténtica o en nombre de este, se utilizará exclusivamente el estado "revocado".

— EAA-6.2.10.1-03.1: Para una lista de estados, esto implica que solo se utilizarán los valores "valid" e "invalid" especificados en la especificación de la lista de estados de *token*.

— EAA-6.2.10.1-03.2: En cuanto a la lista de identificadores, solamente se pondrán en ella los MSO revocados, no los MSO suspendidos temporalmente.

— EAA-6.2.10.1-04: Cuando un MSO esté revocado, estará revocado permanentemente.

— EAA-6.2.10.1-05: La verificación de la lista de revocación de MSO es opcional para la parte usuaria de la cartera y, en su caso, la verificación cumplirá los requisitos de verificación especificados en la especificación de la lista de estados de token y la especificación de la estructura de estado establecida en EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: Cuando una parte usuaria de la cartera necesite poder verificar el estado de revocación de los datos de identificación de la persona o las declaraciones electrónicas de atributos, soportará tanto el mecanismo de lista de estados de declaración como el mecanismo de lista de revocación de declaración establecidos en EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: La identifier_list y la status_list del MSO podrán contener el elemento de certificado.

— EAA-6.2.10.1-06.1: Cuando el elemento de certificado esté presente, contendrá un certificado que contenga la clave pública que firmó o selló el certificado de nivel superior en el elemento x5chain de la estructura de la lista de revocación de MSO.

— EAA-6.2.10.1-06.1.1: La instancia de la parte usuaria de la cartera utilizará dicho certificado como ancla de confianza para la verificación del elemento x5chain en la estructura de la lista de revocación del MSO.

— EAA-6.2.10.1-06.2: Cuando el elemento de certificado no esté presente, el certificado de nivel superior del elemento de x5chain de la estructura de la lista de revocación del MSO irá firmado o sellado por el certificado utilizado para firmar el certificado del elemento x5chain del MSO.

— EAA-6.2.10.1-06.2.1: La instancia de la parte usuaria de la cartera utilizará dicho certificado como ancla de confianza para la verificación del elemento x5chain en la estructura de la lista de revocación del MSO.

— EAA-6.2.10.1-07: Se implementará una lista de revocación del MSO de conformidad con la especificación de lista de estados de *token* como token de lista de estado en formato CWT.

— EAA-6.2.10.1-08: Se aplican los requisitos siguientes en el caso de la lista de revocación del MSO, la lista de identificadores y el mecanismo de la lista de estados:

  — deberá estar presente la declaración exp;

  — puede estar presente la declaración ttl;

  — la declaración aggregation_uri podrá estar presente en la declaración IdentifierList o StatusList y el proveedor de datos de identificación de la persona, el prestador de declaraciones electrónicas cualificadas de atributos o el prestador de declaraciones electrónicas de atributos facilitadas por un organismo del

sector público responsable de una fuente auténtica, o en nombre de este, podrán utilizar la declaración aggregation_uri para indicar el soporte del mecanismo de agregación, según se especifica en la especificación de lista de estados de *token*;

— el CWT será un objeto COSE_Sign1 que utilice uno de los siguientes algoritmos de firma para calcular la firma:

a) "ES256" (ECDSA con curva NIST P-256 y SHA-256);

b) "ES384" (ECDSA con curva NIST P-384 y SHA-384);

c) "ES512" (ECDSA con curva NIST P-521 y SHA-512);

d) "ESB256" (ECDSA con curva brainpoolP256r1 y SHA-256);

e) "ESB384" (ECDSA con curva brainpoolP384r1 y SHA-384);

f) "ESB512" (ECDSA con curva brainpoolP512r1 y SHA-512);

— la CWT contendrá x5chain en la cabecera protegida que contiene el certificado o la cadena de certificados para verificar la firma de la lista de revocación del MSO;

— la utilización ampliada de la clave del identificador de objeto especificado en la especificación de la lista de estados de los *token* podrá emplearse para la lista de estados y el certificado de firma de la lista de identificadores, y las instancias de la parte usuaria de la cartera podrán soportar la utilización ampliada de la clave de los identificadores de objeto especificados en la especificación de la lista de estados de los *token* y, para el identificador del objeto, el prestador de declaraciones electrónicas cualificadas de atributos, o el prestador de declaraciones electrónicas de atributos facilitadas por un organismo del sector público o en su nombre, no deben hacer que el campo de utilización ampliada de la clave sea crítico cuando se emplee la OID de utilización ampliada de clave que se especifica en la especificación de la lista de estados de los *token*.

— EAA-6.2.10.1-09: No obstante los requisitos de la especificación de la lista de estados de los *token*, para el mecanismo de la lista de identificadores se aplican los siguientes requisitos:

— el valor de la declaración type será "application/identifierlist+cwt";

— la declaración StatusList no deberá estar presente en el conjunto de declaraciones CWT;

— la estructura IdentifierList definida en EAA-6.2.10.1-11 deberá estar presente como declaración en las declaraciones CWT establecidas utilizando la clave 65530.

— EAA-6.2.10.1-10: La estructura IdentifierList será una estructura CBOR con la siguiente CDDL:

```
IdentifierList = {

    "identifiers": { * Identifier => IdentifierInfo },

    ? "aggregation_uri": Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: Cuando el identificador de la IdentifierList esté presente, se revoca el MSO que contiene el identificador en el elemento de estado.

— EAA-6.2.10.1-10.2: La declaración Aggregation_uri se especifica en la sección 9.2 de la especificación de la lista de estados de los *token*.

— EAA-6.2.10.1-10.3: El tipo de contenido de la lista de identificadores será “application/identifierlist+cwt” que se establece en los requisitos especificados en la sección 8.2 de la especificación de la lista de estados de los *token*.

— EAA-6.2.10.1-11: Los siguientes requisitos se aplican al elemento identifier_list del MSO (véase EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: El elemento identifier_list será una estructura CBOR con la siguiente CDDL:

```
IdentifierListInfo = {

        "id": Identifier,

        "uri": URI,

        ? "certificate": Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Para evitar que el identificador se utilice como correlación entre presentaciones, este será único por MSO.

— EAA-6.2.10.1-12: Se aplicarán los siguientes requisitos a la lista de estados:

  — EAA-6.2.10.1-12.1: El elemento bits de la estructura StatusList se fijará en 1.

— EAA-6.2.10.1-13: Los siguientes requisitos se aplican al elemento status_list del MSO (véase EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: El elemento status_list cumplirá los requisitos de la estructura StatusListInfo según se indica en la especificación de la lista de estados de los *token* y se añadirá el elemento opcional del certificado definido en EAA-6.2.10.1-06.

  — EAA-6.2.10.1-13.2: Para evitar que el índice de estados sea una correlación entre presentaciones, la combinación del índice de estados y la URI será única por MSO.

— EAA-6.2.10.1-14: El proveedor de cartera utilizará el segundo (EAA-6.2.10.1-02.2) o el tercero (EAA-6.2.10.1-02.3) de los métodos especificados en EAA-6.2.10.1-02 para la revocación de una declaración de instancia de cartera (WIA) y para la revocación de una atestación de clave (KA).

— EAA-6.2.10.1-15: El proveedor de cartera implementará en su solución de cartera los mecanismos de revocación de la certificación especificados en EAA-6.2.10.1-02.

— EAA-6.2.10.1-16: El proveedor de datos de identificación de la persona y el prestador de declaraciones electrónicas de atributos soportarán tanto el mecanismo de lista de estados de declaración como el mecanismo de lista de revocación de declaración especificados en EAA-6.2.10.1-02 para verificar el estado de revocación de una declaración de instancia de cartera (WIA) y de una atestación de clave (KA)

— EAA-6.2.10.1-17: La estructura del estado del MSO será una estructura CBOR con la siguiente CDDL:

```
Status = {
? "identifier_list" : IdentifierListInfo,
? "status_list" : StatusListInfo,
* tstr => RFU
    }».
```

ANEXO V

«ANEXO III

Especificaciones técnicas mencionadas en el artículo 10

— Especificaciones técnicas:

  — Cláusula 4.2.5 de ETSI TS 119 472-3 V1.1.1 (2026-03).».

ANEXO VI

El anexo IV del Reglamento de Ejecución (UE) 2024/2979 se modifica como sigue:

1) el punto 1 se sustituye por el texto siguiente:

«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 V1.2.1 (2024-01); "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures."»;

2) el punto 3 se sustituye por el texto siguiente:

«3. Interfaz de programación de aplicaciones:
ETSI TS 119 432 v1.3.1 (2026-03) cláusulas 6.4.3, A.6, A.7 y A.8.».

ANEXO VII

«ANEXO VI

Etiqueta de confianza de la UE para la cartera de identidad digital en color.

»

ANEXO VIII

«*ANEXO VII*

Etiqueta de confianza de la UE para la cartera de identidad digital en blanco y negro.

»

ANEXO IX

«ANEXO VIII

Datos de la etiqueta de confianza de la UE para la cartera de identidad digital

Datos	Descripción	Codificación	Carácter
TrustMarkResourceURL	URL de los gráficos de la etiqueta de confianza de la UE para la cartera de identidad digital y recursos de información al usuario de la interfaz de usuario de la cartera.	URL	Obligatorio
ListOfCertifiedWalletsURL	URL de la lista pública de soluciones de cartera certificadas en la UE, tal como se establece en el Reglamento de Ejecución (UE) 2025/849 de la Comisión ([1]).	URL	Obligatorio
ListOfCertifiedWalletsURL	Código QR que contiene la información de ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	Opcional
WalletSolutionInfoPageURL	URL a la página de información de la solución de cartera certificada de la lista de la página de soluciones de carteras certificadas de la URL de ListOfCertifiedWalletsURL adjunta con un "?" y el identificador WalletSolutionID de la solución de cartera.	URL	Obligatorio
WalletSolutionInfoPageQRCode	Código QR que contiene la información de WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Opcional
WalletVerifierToolURL*	URL que apunta al punto de conexión (*endpoint*) de /.well-known/openid-credential-issuer de la herramienta de verificación de carteras que se utiliza para la recuperación de los metadatos del expedidor de la declaración.	URL	Opcional

([1]) Reglamento de Ejecución (UE) 2025/849 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 que respecta a la presentación de información a la Comisión y al Grupo de Cooperación para la lista de carteras europeas de identidad digital certificadas (DO L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).».

ANEXO X

El anexo II del Reglamento de Ejecución (UE) 2024/2980 se modifica como sigue:

1) En el anexo II, sección 1, punto 1, la letra i) se sustituye por el texto siguiente:

«i) uno o más certificados que cumplan la norma ETSI EN 319 412-2 V2.4.1 (2025-06) o la norma ETSI EN 319 412-3 V1.3.1 (2023-09) que puedan utilizarse para verificar la firma o el sello creados por el registrador sobre los datos del registro y en los que entre los datos de identidad certificados figuren el nombre del registrador y, cuando proceda, su número de registro, según lo establecido en las letras c) y d), respectivamente.».

2) En el anexo II, sección 2, punto 1, la letra h) se sustituye por el texto siguiente:

«h) uno o varios certificados conformes con la norma ETSI EN 319 412-2 V2.4.1 (2025-06) o la norma ETSI EN 319 412-3 V1.3.1 (2023-09) que puedan utilizarse para autenticar y validar las declaraciones de unidad de cartera que haya expedido el proveedor de cartera y en los que entre los datos de identidad certificados figuren el nombre y, en su caso, el número de registro del proveedor de cartera, según se especifica en las letras a) y b), respectivamente;».

3) En el anexo II, sección 3, punto 1, la letra h) se sustituye por el texto siguiente:

«h) uno o más certificados que cumplan la norma ETSI EN 319 412-2 V2.4.1 (2025-06) o la norma ETSI EN 319 412-3 V1.3.1 (2023-09) que puedan utilizarse para verificar la firma o el sello creados por el proveedor de datos de identificación de la persona sobre los datos de identificación de la persona que proporciona, y en los que entre los datos de identidad certificados figuren el nombre y, cuando proceda, el número de registro del proveedor de datos de identificación de la persona, según lo especificado en las letras a) y b), respectivamente.».

4) En el anexo II, sección 4, punto 1, la letra g) se sustituye por el texto siguiente:

«g) uno o más certificados que cumplan la norma ETSI EN 319 412-2 V2.4.1 (2025-06) o la norma ETSI EN 319 412-3 V1.3.1 (2023-09) que puedan utilizarse para verificar la firma o el sello creados por el proveedor de certificados de acceso de partes usuarias de la cartera sobre el certificado de acceso que proporciona a las partes usuarias de la cartera, acompañados, cuando proceda, de la información necesaria para distinguir los certificados de acceso de partes usuarias de la cartera de otros certificados.».

5) En el anexo II, se añade la sección 5 siguiente:

«5. Notificaciones de información sobre los proveedores de certificados de registro de partes usuarias de la cartera

1. Los Estados miembros facilitarán a la Comisión la siguiente información sobre los proveedores de certificados de registro de partes usuarias de la cartera:

a) el nombre del proveedor de certificados de registro de partes usuarias de la cartera;

b) cuando proceda, un número de registro del proveedor de certificados de registro de partes usuarias de la cartera;

c) el Estado miembro en el que esté establecido el proveedor de certificados de registro de partes usuarias de la cartera;

d) el correo electrónico de contacto y el número de teléfono de contacto del proveedor de certificados de registro de partes usuarias de la cartera, para las cuestiones relacionadas con los certificados de registro que proporciona a dichas partes;

e) cuando proceda, la URL de la página web del proveedor de certificados de registro de partes usuarias de la cartera que contenga información adicional sobre el proveedor y los certificados de registro que proporciona a las partes usuarias de la cartera;

f) la URL de la página web que contenga las políticas y condiciones aplicables al suministro y a la utilización de los certificados de registro que proporciona a las partes usuarias de la cartera;

g) uno o más certificados que cumplan la norma ETSI EN 319 412-2 V2.4.1 (2025-06) o la norma ETSI EN 319 412-3 V1.3.1 (2023-09) que puedan utilizarse para verificar la firma o el sello creados por el proveedor de certificados de acceso de partes usuarias de la cartera sobre el certificado de acceso que proporciona a las partes usuarias de la cartera, acompañados, cuando proceda, de la información necesaria para distinguir los certificados de acceso de partes usuarias de la cartera de otros certificados.

2. La información a que se refiere el punto 1 se facilitará por proveedor de certificados de registro de partes usuarias de la cartera.».

ANEXO XI

«ANEXO I

Protocolos e interfaces a que se refiere el artículo 4

La especificación técnica ETSI TS 119 472-3 V1.1.1 (2026-03) se aplicará con las adaptaciones siguientes:

1) 4.1 General requirements

— GEN-REQ-4.1-05: sin efecto.

— *NOTA*: sin efecto.

2) 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— ISS-MDATA-REG_CERT-4.2.3-04: Uno de los elementos del parámetro *array* issuer_info contendrá el certificado de registro del proveedor de PID/EAA.

— ISS-MDATA-REG_CERT-4.2.3-07: sin efecto.

— ISS-MDATA-REG_CERT-4.2.3-08: sin efecto.

— ISS-MDATA-REG_CERT-4.2.3-09: sin efecto.

— ISS-MDATA-REG_CERT-4.2.3-10: sin efecto.

— ISS-MDATA-REG_CERT-4.2.3-11: sin efecto.

— ISS-MDATA-REG_CERT-4.2.3-12: sin efecto.

— ISS-MDATA-REG_CERT-4.2.3-13: sin efecto.

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Cuando el miembro id tenga el valor “arf_annex_ii” y el *array* asignado a la etiqueta “details” contenga el valor “once_only” o el valor “per-relying-party”, el objeto JSON que contenga este *array* asignado a la etiqueta “details” contendrá también un número JSON asignado a la etiqueta “reissue_trigger_unused”.

4) El anexo A no será aplicable.».

ANEXO XII

«ANEXO II

Especificaciones técnicas mencionadas en el artículo 5

Se aplicará la especificación técnica del anexo C de la norma ISO/IEC 18013-7:2025.

Las especificaciones técnicas de las cláusulas 4.1, 4.2, 5 y 6 de ETSI TS 119 472-2 V1.2.1 (2026-03) se aplicarán con las siguientes adaptaciones, además de la inclusión de una nueva cláusula 4.3:

1) 1 Scope

— El presente documento especifica dos perfiles de protocolos para permitir a las partes usuarias (en lo sucesivo, "RP") solicitar presentaciones de declaraciones electrónicas de atributos (EAAP) o datos de identificación de la persona (en lo sucesivo, "PID") a la cartera europea de identidad digital (EUDI), y a la cartera europea de identidad digital enviar los EAAPs/PIDs solicitados a las RP. Cada uno de los perfiles soporta dos mecanismos de transmisión, a saber: con mediación de API y sin mediación de API, como se muestra a continuación:

a) Un perfil se basa en:

— ISO/IEC 18013-5 [10] únicamente para los mecanismos de transmisión sin mediación de API, y

— en el anexo C de la norma ISO/IEC 18013-7 [16] para el mecanismo de transmisión con mediación de API.

Este perfil se denomina perfil ISO/IEC-mdoc y se define en la cláusula 5 del presente documento.

b) Un perfil se basa en:

OpenID4VC-HAIP [11] para mecanismos de transmisión con mediación de API y sin mediación de API, según se indica:

— las secciones 5, 5.1, 5.3, 7 y 8 de [11] para la transmisión a través de Redirects o de un mecanismo de transmisión sin mediación de API, y

— las secciones 5, 5.2, 5.3, 7 y 8 de [11] para el mecanismo de transmisión con mediación de API.

Este perfil se denomina OpenID4VC-HAIP y se define en la cláusula 6 del presente documento.

2) 2.1 Referencias normativas

— [15] ISO 639: "Language code".

— [16] ISO/IEC 18013-7:2025 "Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions".

3) 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: sin efecto.

4) 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: sin efecto.

— *Nota 2*: sin efecto.

— EAAP-ISO/IEC-mdoc-02: sin efecto.

5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: La cartera europea de identidad digital (cartera EUDI) admitirá una API mediadora que admita tanto los protocolos definidos en la cláusula 5.2 de [11] como en el anexo C de [16].

— *NOTA*: Cuando el dispositivo en el que está instalada la cartera EUDI no admita ambos protocolos, este requisito no podrá cumplirse, lo que dará lugar a una no conformidad debido a que los sistemas operativos subyacentes y los navegadores no implementan las características de interoperabilidad necesarias.

— EAAP-API-GEN-02: La cartera EUDI admitirá una API de mediación al menos para los PID y los tipos de EAA registrados en el catálogo de sistemas, tal como se define en el Reglamento de Ejecución (UE) 2025/1569, y al menos para todos los formatos definidos en el anexo II del Reglamento de Ejecución (UE) 2024/2979.

— *NOTA 1*: Este requisito no podrá cumplirse cuando el sistema operativo subyacente, el navegador, las API intermediarias o cualquier otra capa técnica que quede fuera del control de la cartera EUDI restrinja, filtre, preseleccione o limite de otro modo los formatos de las credenciales, y los tipos de PID y CEA registrados en el catálogo de sistemas. Cuando dicha restricción impida que la cartera EUDI admita un tipo o formato de credencial registrado, la falta de conformidad resultante será atribuible al fracaso de dichos sistemas operativos subyacentes, navegadores, API de mediación u otro nivel técnico pertinente a la hora de proporcionar las características de interoperabilidad necesarias.

6) 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: La cartera EUDI validará el certificado de registro de parte usuaria de la cartera recibido en la solicitud antes de presentar cualquier PID o declaración electrónica de atributos solicitados al usuario de la cartera para su aprobación.

— WRP-VALIDATION-02: Cuando la validación del certificado de registro de parte usuaria de la cartera fracase, incluso cuando el certificado haya expirado, se haya revocado, no haya sido expedido por un proveedor de confianza válido de certificados de registro de parte usuaria de la cartera, esté formado inadecuadamente o no pueda verificarse criptográficamente, la cartera EUDI advertirá al usuario de la cartera de que la parte usuaria de la cartera no ha podido ser validada y no presentará la solicitud como validada satisfactoriamente. El usuario de una cartera aprobará explícitamente la solicitud de la parte usuaria. La falta de respuesta o unas casillas que ya vengan marcadas por defecto no bastarán para una aprobación explícita.

— WRP-VALIDATION-03: El proveedor de la cartera determinará, sobre la base de su análisis de riesgos y su política de seguridad, si el usuario de la cartera puede eludir controles de validación fallidos específicos y en qué condiciones.

— WRP-OVERASKING-01: La cartera EUDI comparará las declaraciones y atributos solicitados por la parte usuaria de la cartera con las declaraciones y atributos registrados en el certificado de registro de parte usuaria de la cartera.

— WRP-OVERASKING-02: Cuando la parte usuaria de la cartera solicite PID o declaraciones electrónicas de atributos o declaraciones que no estén cubiertas por el certificado de registro de parte usuaria de la cartera, la cartera EUDI advertirá claramente al usuario de la cartera antes de cualquier divulgación. La advertencia indicará que la parte usuaria de la cartera solicita más información de la que ha registrado. El usuario de una cartera aprobará explícitamente la solicitud de la parte usuaria. El silencio o unas casillas que ya vengan marcadas no bastarán para una aprobación explícita.

— WRP-OVERASKING-03: El proveedor de una cartera determinará, sobre la base de su análisis de riesgos, su política de seguridad y la legislación aplicable, si el usuario de la cartera puede continuar a pesar de dicha advertencia, si solo puede divulgarse el subconjunto de datos solicitados cubiertos por el certificado de registro o si se rechazará la solicitud.

7) 5.1 Introduction

— La cláusula 5 y sus subcláusulas definen un perfil para un protocolo que permite a una RP solicitar EAAPs o PIDs a la cartera europea de identidad digital, y a la cartera europea de identidad digital enviar los EAAPs/PIDs solicitados a la RP utilizando un mecanismo de transmisión sin mediación de API, basado en la norma ISO/IEC 18013-5 [10], o un mecanismo de transmisión con mediación de API basado en el anexo C de la norma ISO/IEC 18013-7 [16] para transferir las estructuras de datos definidas en la norma ISO/IEC 18013-5 [10] adecuadamente encapsuladas.

— El resto de la cláusula 5 se organiza de la siguiente manera:

  — la cláusula 5.2 define los requisitos relativos al soporte del perfil y los mecanismos de transmisión por parte de las RP y la cartera europea de identidad digital;

  — la cláusula 5.3 especifica los requisitos específicos para el mecanismo de transmisión sin mediación de API;

  — la cláusula 5.4 y sus subcláusulas especifican requisitos específicos para el mecanismo de transmisión con mediación de API.

8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Las unidades de cartera, los proveedores de PID, los proveedores de declaraciones, los proveedores de carteras y las partes usuarias no soportarán la recuperación de servidores, según se especifica en la norma ISO/IEC 18013-5 [10], para solicitar y presentar atributos de declaración o PID.

— ISO/IEC 18013-SUPPORT-02: La cartera europea de identidad digital cumplirá los requisitos establecidos en las cláusulas 5.3 y 5.4 del presente documento.

— ISO/IEC 18013-SUPPORT-04: Una parte usuaria debe implementar el perfil definido en la cláusula 5.4 del presente documento.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Las solicitudes de productos enviadas a las carteras europeas de identidad digital contendrán el par clave-valor “requestInfo” especificado en la cláusula 8.3.2.1.2.1 de [10]. El valor de este par será del tipo RequestInfo.

— ISO/IEC 18013-5-REQ-05: El tipo RequestInfo se ajustará a la definición de CDDL que figura a continuación.

```
RequestInfo = {

    'euWrprc': bstr ; contiene un certificado de registro (ver los requisitos más adelante)

}
```

— ISO/IEC 18013-5-REQ-06: El mencionado miembro de requestInfo contendrá un miembro con la etiqueta “euWrprc”.

— ISO/IEC 18013-5-REQ-07: El valor de “euWrprc” será un certificado de registro codificado en CBOR.

— ISO/IEC 18013-5-REQ-08: sin efecto.

— *NOTA 3*: sin efecto.

— ISO/IEC 18013-5-REQ-09: sin efecto.

— ISO/IEC 18013-5-REQ-10: sin efecto.

— ISO/IEC 18013-5-REQ-11: sin efecto.

10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— La presente cláusula define los requisitos para el tipo de mensaje DeviceResponse, común a los dos tipos de mecanismos de transmisión (con mediación de API y sin mediación de API).

— *NOTA 1*: Cuando se utiliza un mecanismo sin mediación de API basado en la norma ISO/IEC 18013-5 [10], una respuesta EAAP es exactamente una instancia de DeviceResponse, tal como se describe en la presente cláusula. Cuando se utiliza un mecanismo con mediación de API basado en el anexo C de la norma ISO/IEC 18013-7 [16], la instancia de DeviceRequest se encapsula según se especifica en el anexo C de [16].

— ISO/IEC 18013-5-RESP-02: El proveedor de datos de identificación de la persona y declaraciones electrónicas de atributos no incluirá ningún elemento de datos en el mapa de KeyAuthorizations en el objeto de seguridad móvil de los datos de identificación de la persona y las declaraciones electrónicas de atributos que expida, excepto en el caso de los elementos de datos facilitados por la parte usuaria de la cartera en los datos transaccionales de la petición mdoc que debe firmar o sellar la unidad de cartera utilizando la clave privada de los datos de identificación de la persona o las declaraciones electrónicas de atributos.

— *NOTA 2*: En consecuencia, las unidades de cartera no pueden presentar a las partes usuarias de la cartera ningún elemento de datos firmado por el dispositivo, excepto para firmar datos que la parte usuaria de la cartera haya facilitado, por ejemplo en casos de uso para la autenticación segura del usuario.

— *NOTA 3*: La norma ISO/IEC 18013-5:2021 no especifica cómo las partes usuarias de la cartera pueden incluir datos transaccionales en una petición mdoc. La inclusión de datos transaccionales en una petición mdoc se llevará a cabo con el añadido de especificaciones técnicas.

— ISO/IEC 18013-5-RESP-03: Los proveedores de datos de identificación de la persona no permitirán que la clave privada de los datos de identificación de la persona firme elementos de datos facilitados por la parte usuaria de la cartera en los datos de transacción de la petición mdoc.

11) 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

La presente cláusula define los requisitos para los mecanismos de transmisión con mediación de API en relación con los requisitos definidos en el anexo C de [16].

— ISO/IEC 18013-7-API-01: El perfil que soporta las presentaciones con mediación de API deberá cumplir los requisitos del anexo C de la norma ISO/IEC 18013-7 [16], tal como se definen en las cláusulas 5.3 y 5.4 del presente documento.

— ISO/IEC 18013-7-API-02: Todos los requisitos obligatorios definidos en el anexo C de [16] se aplicarán según se definen en las cláusulas 5.3 y 5.4 del presente documento.

— ISO/IEC 18013-7-API-03: Todos los requisitos opcionales definidos en el anexo C de [16] seguirán siendo opcionales, salvo que se indique lo contrario en el presente documento.

12) 5.4.2 Additional requirements

— La presente cláusula especifica requisitos adicionales para los mecanismos de transmisión con mediación de API.

— ISO/IEC 18013-ADD-API-01: La cartera europea de identidad digital divulgará por defecto la presencia de todas las declaraciones electrónicas almacenadas del tipo de atributos a la API mediadora que funcione de conformidad con el anexo C de [16], pero no revelará los atributos ni sus valores en estas declaraciones electrónicas de atributos.

— *NOTA 1*: La restricción del valor de los atributos se aplica incluso si dicha divulgación mejorara los servicios prestados por el sistema operativo a la cartera europea de identidad digital, por ejemplo, la selección de la declaración en el contexto de la API mediadora.

— Hay asuntos relacionados con los sistemas operativos y los navegadores que escapan al control de los implementadores que pueden tenerse en cuenta como se indica en las siguientes notas 2 a 4:

— *NOTA 2*: El navegador o el sistema operativo pueden procesar una petición de presentación de una parte usuaria que soporte el anexo C de [16] para buscar EAA disponibles, prevenir el fraude dirigido al usuario o resolver problemas.

— *NOTA 3*: Se espera que el navegador o el sistema operativo procesen, a efectos de seguridad de los usuarios, una petición de presentación de una parte usuaria que soporte el anexo C de [16].

— *NOTA 4*: Se espera que el navegador o el sistema operativo no procesen una petición de presentación de una parte usuaria que soporte el anexo C de [16] con fines de análisis del mercado (también como finalidad secundaria) o para fines internos del navegador o del sistema operativo.

— ISO/IEC 18013-ADD-API-02: Cuando una cartera europea de identidad digital suprima, a petición del usuario, un PID o una EAA previamente divulgados a la API mediadora que funcione de conformidad con el anexo C de [16], la cartera europea de identidad digital revelará a la API de mediación el que ya no almacena este PID o EAA.

— ISO/IEC 18013-ADD-API-03: Si el usuario desinstala su cartera europea de identidad digital, esta revelará el hecho de que ya no almacena ningún PID o EAA divulgados previamente a la API mediadora que funciona de conformidad con el anexo C de [16].

— ISO/IEC 18013-ADD-API-04: La cartera europea de identidad digital proporcionará un ajuste de usuario global para desactivar la divulgación de EAA almacenadas a través de una API mediadora que funcione como se especifica en la norma ISO/IEC 18013-ADD-API-01. Cuando este ajuste esté desactivado, la cartera europea de identidad digital no anunciará ni responderá a las peticiones de presentación o de expedición con mediación de API.

— ISO/IEC 18013-ADD-API-05: Las carteras EUDI verificarán, en los flujos entre dispositivos y utilizando la API mediadora, que el dispositivo que interactúa esté muy cerca físicamente de la cartera EUDI mediante un canal de comunicación local seguro, directo y mediado por el usuario, como una tecnología de comunicación inalámbrica de corto alcance a fin de llevar a cabo la comprobación de proximidad física.

— *NOTA*: El CTAP 2.3 permite utilizar BLE para realizar la comprobación de la proximidad física y, cuando lo implementan ambos dispositivos, también permite transportar los datos entre los dispositivos a través de tecnologías de transmisión de corto alcance. La realización tanto de la comprobación de la proximidad física como de la transferencia de datos entre los dos dispositivos utilizando un canal de comunicación local habilitado por el CTAP 2.3 debe preferirse a los sistemas operativos subyacentes, los navegadores, las API mediadoras o cualquier otra capa técnica que escape al control de la cartera EUDI sobre el uso de los servicios de túnel híbrido del CTAP.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: La cartera europea de identidad digital deberá cumplir los requisitos especificados en la cláusula 6.5 del presente anexo.

— OIDFVP-HAIP-SUPPORT-03: La cartera europea de identidad digital no deberá soportar el mecanismo basado en redirecciones especificado en la cláusula 6.4 para los flujos de presentación entre dispositivos.

— *NOTA 3*: El uso de este mecanismo es vulnerable a ataques, como los de fijación de la sesión. La mitigación de estos ataques corresponde a las partes usuarias. La aplicación de este mecanismo no debe dar lugar a incumplimientos.

— OIDFVP-HAIP-SUPPORT-05: Una parte usuaria deberá cumplir los requisitos especificados en la cláusula 6.5 del presente anexo.

— *NOTA 5*: sin efecto.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: Se aplicarán todos los requisitos obligatorios especificados en las cláusulas 5, 5.3, 7 y 8 de HAIP [11].

— *NOTA 1*: "HAIP [11], Sección 5" se refiere únicamente a los requisitos que figuran directamente bajo el título de la sección 5. No se incluyen las secciones 5.1, 5.2 ni 5.3.

— OIDFVP-HAIP-GEN-03: Si el presente anexo modifica un requisito de OpenID4VC-HAIP [11], prevalecerá el requisito modificado especificado en el presente anexo.

— *NOTA 2*: Esto permitiría, por ejemplo, convertir en obligatorio un requisito opcional de OpenID4VC-HAIP [11] o ampliar los requisitos obligatorios.

— OIDFVP-HAIP-GEN-04: Cuando el formato de la declaración solicitada cumpla lo dispuesto en [10] las partes usuarias y las carteras europeas de identidad digital se ajustarán al perfil "ISO mdocs" de [11], sección 6.

— *NOTA 3*: En aras de la claridad: el "perfil ISO mdocs" de HAIP implica que las partes usuarias y las carteras europeas de identidad digital deben cumplir los requisitos aplicables de [7], anexo B.2.

— OIDFVP-HAIP-GEN-05: Cuando el formato de la declaración solicitada se ajuste a [2], las partes usuarias y las carteras europeas de identidad digital se ajustarán al perfil "IETF SD-JWT VCs" en [11], sección 6.

— *NOTA 4*: En aras de la claridad: el "perfil IETF SD-JWT VCs" implica que las partes usuarias y las carteras europeas de identidad digital deben cumplir los requisitos de [7], anexo B.3, así como los requisitos de [11], sección 6.1.

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: sin efecto.

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-03: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-04: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-05: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-06: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-07: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-08: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-09: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-10: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-11: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-12: sin efecto.

— *Nota 2*: sin efecto.

— OIDFVP-HAIP-COMMON-REQ-RO-13: Uno de los elementos del parámetro verifier_info incluirá el certificado de registro.

— OIDFVP-HAIP-COMMON-REQ-RO-23: El certificado de hoja mencionado en OpenID4VP, sección 5.9.3, para su uso con el x509_hash Client Identifier Prefix será un certificado de acceso de RP según se especifica en ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: sin efecto.

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: sin efecto.

— *NOTA*: sin efecto.

19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: La cartera europea de identidad digital revelará por defecto la presencia de todos los tipos de EAA almacenados a la API mediadora que funcione de conformidad con la cláusula 5.2 de [11], pero no revelará los atributos ni sus valores en esas EAA.

— OIDFVP-HAIP-ADD-API-04: Si la cartera europea de identidad digital soporta una API mediadora que funcione como se especifica en OIDFVP-HAIP-ADD-API-01, proporcionará un ajuste de usuario global para desactivar la divulgación de las EAA almacenadas a través de la API mediadora. Cuando este ajuste desactive la divulgación, la cartera europea de identidad digital debe permitir posteriormente al usuario seleccionar declaraciones concretas que deben divulgarse a la API mediadora.

— OIDFVP-HAIP-ADD-API-05: Las carteras EUDI verificarán en los flujos entre dispositivos, utilizando la API mediadora, que el dispositivo que interactúa esté muy cerca físicamente de la cartera EUDI mediante un canal de comunicación local seguro, directo y mediado por el usuario, como una tecnología de comunicación inalámbrica de corto alcance a fin de llevar a cabo la comprobación de proximidad física.

— *NOTA 5*: El CTAP 2.3 permite utilizar BLE para realizar la comprobación de la proximidad física y, cuando lo implementen ambos dispositivos, también permite transportar los datos entre los dispositivos a través de tecnologías de transmisión de corto alcance. La realización tanto de la comprobación de la proximidad física como de la transferencia de datos entre los dos dispositivos utilizando un canal de comunicación local habilitado por el CTAP 2.3 debe preferirse a los sistemas operativos subyacentes, los navegadores, las API mediadoras o cualquier otra capa técnica que escape al control de la cartera EUDI sobre el uso de los servicios de túnel híbrido del CTAP.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Todos los requisitos especificados en el presente documento aplicables a las estructuras de petición de dispositivo y respuesta de dispositivo especificadas en la norma ISO/IEC 18013-5 también se aplican cuando la cartera europea de identidad digital reciba una petición de presentación ISO/IEC mdoc a través de un mecanismo transmitido por API especificado en la cláusula C.1 de [16].».