Cartera de Identidad Digital Europea

Arquitectura y marco de referencia

v1.8.0 20250327.111202

Versión en español generada el 5 de abril de 2025 por Julián Inza (**EAD Trust**)

Contenido

Contenido

Arquitectura y marco de referencia

1 Introducción

1.1 Contexto

El 3 de junio de 2021, la Comisión Europea adoptó una Recomendación ([REC- OMENDACIÓN DE LA COMISIÓN (UE) 2021/946 de 3 de junio de 2021 sobre una caja de herramientas común de la Unión para un enfoque coordinado hacia un Marco Europeo de Identidad Digital, DO L 210/51 de 14.6.2021) en la que pedía a los Estados miembros que colaboraran estrechamente con la Comisión en el desarrollo de una caja de herramientas que incluyera una arquitectura técnica y un marco de referencia (en lo sucesivo, el ARF), un conjunto de normas comunes y especificaciones técnicas y un conjunto de directrices comunes y mejores prácticas.

La Recomendación especifica que estos resultados servirán de base para la aplicación del [Reglamento Europeo de Identidad Digital], sin que el proceso de desarrollo de la caja de herramientas interfiera o prejuzgue el proceso legislativo.

La Recomendación establece un marco estructurado para la cooperación entre los Estados miembros, la Comisión y, en su caso, los operadores del sector privado para desarrollar la caja de herramientas. El Grupo Europeo de Cooperación en materia de Identidad Digital (EDICG), anteriormente conocido como Grupo de Expertos eIDAS, es responsable de:

- intercambiar buenas prácticas y cooperar con la Comisión en las nuevas iniciativas políticas en el ámbito de las carteras de identidad digital, los medios de identificación electrónica y los servicios de confianza;
- asesorar a la Comisión en la preparación de proyectos de actos de ejecución y actos delegados; • apoyo a los organismos de supervisión en la aplicación del [Reglamento Europeo de Identidad Digital];
- organizar revisiones inter pares de los sistemas de identificación electrónica;
- colaborar con la Comisión y otras partes interesadas para desarrollar una caja de herramientas de la Unión;común

La página del Grupo Europeo de Cooperación en materia de Identidad Digital puede consultarse en la página oficial.

Desde entonces, el Grupo Europeo de Cooperación en materia de Identidad Digital ha seguido desarrollando los conceptos y especificaciones del Marco Europeo de Identidad Digital. La versión actual del ARF se basa en el texto legal adoptado por los colegisladores, incluidos los Reglamentos de Ejecución de la Comisión adoptados:

- CIR 2024/2977 sobre DIP y DEA,
- CIR 2024/2979 sobre integridad y funcionalidades básicas,
- CIR 2024/2980 sobre notificaciones de ecosistemas,
- CIR 2024/2981 relativo a la certificación de Soluciones Cartera,
- CIR 2024/2982 sobre protocolos e interfaces.

1.2 Objeto del presente documento

El propósito de este documento es explicar la arquitectura del ecosistema Cartera IDUE y todos sus componentes, así como la forma en que estos componentes interactuarán para garantizar la seguridad del ecosistema y la privacidad de sus Usuarios. Además, sirve como información de fondo para permitir una mejor comprensión de los requisitos de alto nivel establecidos en el Anexo 2.

Además, este documento constituye una referencia para crear condiciones uniformes para la aplicación del [Reglamento Europeo de Identidad Digital] y para definir las especificaciones técnicas, normas y procedimientos que la Comisión desarrollará con el fin de aplicar este Reglamento.

Por último, este documento se utiliza para desarrollar la implementación de referencia de. la Solución Cartera

El documento presenta el estado de los trabajos en curso del Grupo Europeo de Cooperación en materia de Identidad Digital y no implica ningún acuerdo formal sobre su contenido. Este documento se complementará y actualizará con el tiempo a través del proceso de creación de la caja de herramientas, tal y como se describe en el Capítulo 8.

Este documento no tiene valor legal y no prejuzga los requisitos legales obligatorios finales para el ecosistema Cartera IDUE. Sólo son obligatorios el [Reglamento Europeo de Identidad Digital] adoptado y los actos de ejecución y delegados adoptados en virtud de dicho Reglamento. El presente documento sirve de base para la actualización periódica de los actos de ejecución, garantizando su adaptación a la evolución tecnológica y normativa.

1.3 Relación con los Grandes-Proyectos-Piloto (GPP)

Para apoyar el desarrollo de una implementación de referencia de una solución Cartera IDUE y pilotar su uso en diferentes casos de uso prioritarios, la Comisión lanzó una convocatoria de propuestas el 22 de febrero de 2022 en el marco del Programa Europa Digital para pilotar casos de uso del ecosistema Cartera IDUE a gran escala.

El objetivo de la convocatoria de Grandes-Proyectos-Piloto (GPP) es apoyar el pilotaje del ecosistema Cartera IDUE en torno a una serie de casos de uso en los que participen interesados tanto del sector público como del privado. Los GPP pondrán a prueba el ecosistema Cartera IDUE tanto en contextos nacionales como transfronterizos y se integrarán en el desarrollo iterativo de la aplicación de referencia.

Los trabajos de los GPP se alinearán con el ARF, que guiará el diseño del sistema piloto y el desarrollo de la arquitectura junto con la publicación de la implementación de referencia.

Se espera que los GPP aporten sus comentarios sobre el ARF a medida que desarrollen e interactúen con los servicios de la Parte usuaria, los Prestadores de Declaraciones Electrónicas Cualificadas de Atributos DECA, los Prestadores de Datos de identificación de personas (DIP), los Prestadores de servicios de confianza cualificados y no cualificados y los Usuarios en interacciones significativas según los casos de uso propuestos.

1.4 Definiciones

Las definiciones utilizadas en este documento figuran en el Anexo 1 del mismo.

1.5 Alcance

El documento **Arquitectura y Marco de Referencia (ARF) de Cartera** IDUE define los aspectos estructurales y funcionales del ecosistema de Cartera IDUE, detallando sus componentes clave y sus interacciones. Proporciona una base técnica para garantizar **la interoperabilidad, la seguridad y la privacidad**, en consonancia con los requisitos de alto nivel especificados en **el Anexo 2**. El ARF sirve de referencia para la **aplicación armonizada del [Reglamento Europeo Identidad Digital]**, guiando el desarrollo de **especificaciones técnicas, normas y procedimientos operativos**.

Este documento **sólo se aplica a los ecosistemas de Cartera IDUE que cumplen con el [Reglamento Europeo de Identidad Digital]**, garantizando la coherencia en la arquitectura y la implementación. Está diseñado para apoyar el desarrollo de la implementación de referencia de la Solución Cartera, al tiempo que se mantiene adaptable a los avances tecnológicos y normativos.

1.6 Registro de cambios

En esta versión del ARF,

- En las secciones 6.6.2.7 y 6.6.3.4 . se incluyó el texto pertinente del documento de debate para el Tema D (Políticas de divulgación incorporadas) Los requisitos de alto nivel introducidos en este documento de debate se incluyeron en el Anexo 2 del Tema 43.
- En la sección 6.5.3.4 se incluyó el texto pertinente del documento de debate sobre el tema C (declaración de la unidad Cartera), así como en otras secciones. Sin embargo, sólo se introdujeron cambios limitados. Los requisitos de alto nivel introducidos y modificados en este documento de debate se incluyeron en el anexo 2 del tema 9. Otros requisitos de alto nivel que solían estar en el Tema 9 se trasladaron a otro lugar, principalmente al Tema 40.

- En la sección 7.4.3.5.3 se ha incluido el texto pertinente del documento de debate del Tema G (Pruebas de conocimiento cero). Los requisitos de alto nivel introducidos en este documento de debate se incluyeron en el Anexo 2 del Tema 53.
- En la sección 5.4 se ha incluido el texto pertinente del documento de debate sobre el tema V (Directrices de elaboración de los DIP. Además, en las Directrices de elaboración se han añadido requisitos de alto nivel y una especificación de la codificación y el formato de los DIP basados en [SD-JTW VC

Aparte de estos cambios, se ha corregido un número limitado de errores de redacción.

1.7 Temas adicionales

En esta versión del ARF, varias áreas clave aún requieren mayor exploración y refinamiento. Estos temas se debatirán en colaboración con los Estados miembros, el Grupo Europeo de Cooperación en materia de Identidad Digital, la sociedad civil, los representantes de la industria y los profesionales, con el fin de garantizar una información exhaustiva de todas las partes interesadas. Los resultados de estos debates se incorporarán a futuras versiones de este ARF. El documento se actualizará de forma iterativa para mejorar su contenido y abordar los temas que vayan surgiendo. En el capítulo 8 .se describe el proceso para enviar comentarios y los detalles sobre cómo se gestionarán las actualizaciones

Entre las áreas identificadas para un mayor debate se encuentran:

- Registro de la Parte usuaria (informada).

Otros temas que se desarrollarán son:

- registros de transacciones mantenidos por la Unidad Cartera,

escenarios en los que una persona física representa a otra persona física,

- Interacciones entre Carteras,
- presentaciones combinadas de declaraciones,
- Solicitudes de supresión de datos por Parte usuaria (informada),
- mecanismos para que los usuarios informen de solicitudes de datos ilegales o sospechosas a las autoridades de protección de datos (APD),
- portabilidad de los datos.

En los debates posteriores se explorarán los siguientes temas:

- la elaboración de catálogos de declaraciones,
- interfaces criptográficas seguras entre la Instancia Cartera y la WSCA,
- Interfaces de usuario con instancias de Cartera,
- mecanismos de autenticación para que los usuarios accedan a sus dispositivos,
- transparencia de los certificados,
- responsabilidades de apoyo y mantenimiento de los Prestadores de Cartera,
- el Sello de Confianza Cartera IDUE,
- datos transaccionales que necesitan las Unidades Cartera en los pagos y otros casos de uso.

Una lista detallada de estos temas y el progreso de su desarrollo está disponible en GitHub.

2 Funcionalidades de la Cartera IDUE

2.1 Introducción

El ecosistema de la Cartera IDUE está diseñado como un entorno digital seguro y controlado por el Usuario que le permite utilizar su Unidad Cartera para gestionar y presentar sus datos de identificación personal (DIP) y declaraciones en los servicios públicos y privados de la UE. Sus funcionalidades se basan en la seguridad, la privacidad y el control del usuario, garantizando interacciones fluidas con las Partes usuarias (informadas) y otras entidades, al tiempo que se adhiere a los principios de protección de datos.

En este capítulo se describen las principales funcionalidades de las Soluciones Cartera, tal y como se definen en el [Reglamento Europeo de Identidad Digital], y se examina cómo los requisitos para su implementación se alinean con los casos de uso en el mundo real en los que los Usuarios utilizarán su Unidad Cartera.

Las funcionalidades de una Unidad Cartera pueden agruparse en las siguientes categorías:

- **Identificación y autenticación seguras**, garantizando que los usuarios puedan presentar datos de identificación de personas en un entorno de confianza.

  Intercambio de atributos de usuario cualificados y no cualificados mediante declaraciones electrónicas de atributos seguras y verificables.

- **Firma electrónica de documentos o datos**, que permite a los usuarios crear firmas y sellos electrónicos reconocidos legalmente.
- **Generar y utilizar seudónimos** para la autenticación, con el fin de mejorar la privacidad y evitar el rastreo.

Estas funcionalidades se analizan en las cuatro secciones siguientes.

2.2 Identificación y autentificación

Utilizando sus Unidades Cartera, los Usuarios pueden:

- **Identificar y autenticar** a los servicios en línea y fuera de línea, mientras que el uso **selectivo discierre** de atributos, así como la **aprobación del** usuario. Esto *garantiza que solo se presenten a* las Partes usuarias *los atributos necesarios y aprobados por el usuario*, lo que minimiza la exposición de información personal.
- **Autenticar de forma segura a las Partes usuarias (informadas) u otras Unidades de Cartera**, asegurándose de que los at- tributos sólo se presentan a entidades de confianza.
- **Conéctese sin problemas a los Prestadores de DIP o a los Prestadores de declaraciones** aprovechando los sistemas de identificación electrónica existentes, para un proceso de registro fluido y seguro.
- **Ser informada** de si una Parte usuaria está autorizada o registrada para recibir los atributos solicitados.
- **Acceder a un registro de transacciones a través de un panel de control**, que permite a los usuarios:
  - **Revisar interacciones pasadas** con Partes usuarias (informadas) y Unidades Carteras.
  - **Solicitar la supresión de datos** en virtud del artículo 17 del GDPR para mantener la privacidad.
  - **Notificar las Partes usuarias (informadas) sospechosas** a la autoridad nacional de protección de datos competente.

2.3 Mecanismo de intercambio de atributos mediante declaraciones

Utilizando sus Unidades Cartera, los Usuarios pueden:

Solicitar, almacenar y presentar datos de identificación personal y declaraciones electrónicas de Atributos bajo su exclusivo control, garantizando un uso seguro tanto en línea como fuera de línea.

- **Copia de seguridad de una lista de sus atributos, declaraciones y configuraciones**, garantizando el cumplimiento de los derechos de portabilidad de datos.
- **Evitar el rastreo por Parte usuaria (informada**) al utilizar declaraciones, garantizando interacciones que preserven la privacidad.

2.4 Firma Electrónica Cualificada

Utilizando sus Unidades Cartera, los Usuarios pueden:

- **Cree firmas electrónicas Cualificadas y sellos** para transacciones digitales legalmente vinculantes.
- **Firmar documentos utilizando firmas electrónicas Cualificadas**, que se proporcionan por defecto y de forma gratuita dentro de la Unidad Cartera, garantizando la accesibilidad universal y el cumplimiento de las normas legales.

Estas funcionalidades se implementan utilizando las capacidades de autenticación y firma de la Unidad Cartera como parte de un QSCD local, o un QSCD remoto gestionado por un QTSP. Véanse los Temas 37.16 y

2.5 Seudónimos

Los seudónimos pueden utilizarse para autenticar a un usuario cuando no es necesario que una Parte usuaria (informada) conozca la identidad del . Como se especifica en [CIR 2024/2979], [W3C WebAuthn] define la especificación técnica para pseudónimos. Las claves de paso son un tipo de credencial ampliamente utilizado que se crea y afirma utilizando la API WebAuthn. La sección 4.7 ofrece más información sobre la arquitectura y los flujos de mensajes de las Passkeys.

Un usuario utiliza un seudónimo cuando desea crear una cuenta en una Parte usuaria (informada) sin identificarse. La Parte usuaria (informada) asocia el seudónimo a la cuenta, de modo que pueda utilizarse para la autenticación posterior en interacciones posteriores con esa Parte usuaria. Además, el usuario puede presentar atributos de un DIP o una declaración a la Parte usuaria, ya sea durante el registro del seudónimo o en una interacción posterior.

Véase también el Tema 11 y el Documento de debate sobre el Tema E.

2.6 El papel de los casos de uso en el desarrollo de la Arquitectura y el Marco de Referencia

2.6.1 Visión general

El desarrollo del Marco de Arquitectura y Referencia (ARF) está impulsado estratégicamente por casos de uso del mundo real, garantizando que la experiencia del usuario, la propuesta de valor y los requisitos del ecosistema de Cartera IDUE se aborden de forma eficaz. Para lograrlo, el Grupo Europeo de Cooperación en materia de Identidad Digital creó inicialmente modelos de servicio para cada caso de uso, en los que se detallan los puntos de contacto, los componentes y los procesos del servicio.

Estos anteproyectos cumplen una doble función: desempeñan un papel crucial en el diseño del servicio, mejorando tanto la experiencia del usuario como la eficiencia operativa, al tiempo que identifican áreas de mejora. Como elemento fundacional, estos planos dan forma al desarrollo de especificaciones comunes, proporcionando soluciones completas pero flexibles que pueden dar cabida a enfoques alternativos y pasos opcionales.

Es importante tener en cuenta que los itinerarios de los usuarios pueden variar en función del enfoque de aplicación específico, lo que influye en aspectos como la recuperación de datos y los procesos de aprobación de los usuarios. Los anexos contienen descripciones detalladas de estos modelos, lo que garantiza su transparencia y adaptabilidad.

El Grupo Europeo de Cooperación en Identidad Digital ha esbozado modelos de servicio para los siguientes casos de uso clave:

- Identificación y autenticación para acceder a los servicios en línea, véase la sección 2.6.2,
- Firma Electrónica Cualificada, véase el apartado 2.4,
- Permiso de conducir móvil, véase el apartado 2.6.3,
- Casos de uso adicionales que se introducirán en el , véase la sección 2.6.4.

Estos planos, junto con toda la información pertinente sobre la aplicación de los casos de uso, se recopilarán en un formato normalizado dentro de un documento específico titulado "Manual de casos de uso", y se distribuirán junto con el presente documento.

2.6.2 Identificación y autenticación para acceder a los servicios en línea

El ecosistema de la Cartera IDUE está diseñado principalmente para facilitar la identificación y autenticación seguras de los usuarios a un Nivel de Aseguramiento (LoA) alto para diversos servicios en línea, tanto públicos como privados. Esta capacidad es crucial, ya que permite a las Partes usuarias (informadas) verificar con confianza la identidad de los usuarios con los que interactúan.

En este caso de uso, un usuario utiliza su Unidad Cartera para presentar atributos específicos a una Parte usuaria (informada) con el fin de acceder a servicios en línea. Antes de hacerlo, la Unidad Cartera autentica al . El usuario es especialmente consciente de las implicaciones para la privacidad y la seguridad de compartir datos cuando accede a servicios en línea. Su principal objetivo es acceder de forma segura y fiable a los

servicios en línea que requieren autenticación, manteniendo al mismo tiempo un control total sobre cómo se presentan y comparten sus datos personales.

2.6.3 Permiso de conducción móvil

Un caso de uso significativo para la Unidad Cartera consiste en permitir a los Usuarios solicitar, almacenar y presentar un Carné de Conducir Móvil (mDL) como declaración en su Unidad Cartera, lo que les principalmente demostrar sus privilegios de conducción. En este caso, el usuario utiliza una Unidad Cartera para presentar un Carné de Conducir Móvil a una Parte usuaria (informada), por ejemplo, un agente de policía.

La descripción del caso de uso se centra en los flujos de proximidad supervisada y no supervisada, que implican escenarios en los que el Usuario está físicamente cerca de una Parte usuaria, y el intercambio de atributos mDL se produce utilizando tecnologías de proximidad (por ejemplo, NFC, Bluetooth). Los dos flujos de proximidad tienen una diferencia significativa: en el flujo supervisado, la Unidad de Cartera presenta atributos mDL a una Parte usuaria humana o bajo su supervisión, mientras que en el flujo no supervisado, la Unidad de Cartera presenta atributos mDL a una máquina sin supervisión humana.

Además, como cualquier otro tipo de declaración, el Carné de Conducir Móvil (CCm) puede presentarse en línea, a través de la red.

2.6.4 Otros casos de uso

2.6.4.1 Datos sanitarios

El fácil acceso a los datos sanitarios es crucial tanto en contextos nacionales como transfronterizos. Una unidad Cartera puede permitir el acceso al resumen del paciente, las recetas electrónicas, etc.

2.6.4.2 Declaraciones de estudios y cualificaciones profesionales

Proporcionar credenciales para los procedimientos de reconocimiento de cualificaciones puede ser costoso y llevar mucho tiempo a los Usuarios, Partes usuarias (como empresas y empleadores) y Prestadores de servicios de certificación (como proveedores de educación y formación o instituciones académicas). Una unidad Cartera

puede ser un depósito de credenciales educativas y un medio para que el las presente a las Partes usuarias (informadas) pertinentes.

2.6.4.3 Finanzas digitales

Una unidad Cartera puede facilitar el cumplimiento de los requisitos de autenticación fuerte de clientes, utilizando las capacidades de autenticación de usuarios descritas en la sección 2.6.2. En consonancia con la

Estrategia de Pagos Minoristas de la Comisión, este caso de uso se desarrollaría en estrecha coordinación con los grupos consultivos de los Estados miembros sobre pagos minoristas y el sector financiero.

2.6.4.4 Pasaporte

Los Prestadores de Credenciales de Viaje Digitales (DTC) pueden emitir DTC a las Unidades de Cartera en un formato compatible, para permitir a las Partes usuarias identificar a los Usuarios, facilitando así una experiencia de viaje fluida y el viaje del Usuario. Las Partes usuarias de una DTC pueden ser gobiernos, proveedores de transporte, agentes de hostelería o cualquier otro agente que opere en un entorno regulado que requiera el uso de una DTC.

2.6.4.5 Seguridad Social

Los documentos relacionados con la seguridad social son importantes para que muchos ciudadanos de la UE demuestren sus derechos y obligaciones con arreglo a la legislación de la seguridad social en la UE. Algunos ejemplos son:

- **Documento portátil ("PDA1"**) Se trata de una declaración de la legislación aplicable que se utiliza para demostrar que una persona paga cotizaciones sociales en otro país de la UE, por ejemplo si es un trabajador desplazado o trabaja en varios países al mismo tiempo.
- **Tarjeta Sanitaria Electrónica ("TSE**") Se trata de una tarjeta gratuita que proporciona a todo ciudadano acceso a la asistencia sanitaria pública médicamente necesaria durante una estancia temporal en uno de los 27 países de la UE, Islandia, Liechtenstein, Noruega y Suiza, en las mismas condiciones y al mismo coste (gratuito en algunos países) que las personas aseguradas en ese país. Esto incluye, por ejemplo, servicios relacionados con enfermedades crónicas o existentes, así como en relación con el embarazo y el parto.

3. Ecosistema Cartera IDUE

3.1 Introducción

Este capítulo describe el ecosistema de Carteras IDUE tal y como está previsto en el [Reglamento Europeo de Identidad Digital]. Las distintas funciones del ecosistema Cartera IDUE se describen en la Figura 1 y se detallan en las secciones siguientes.

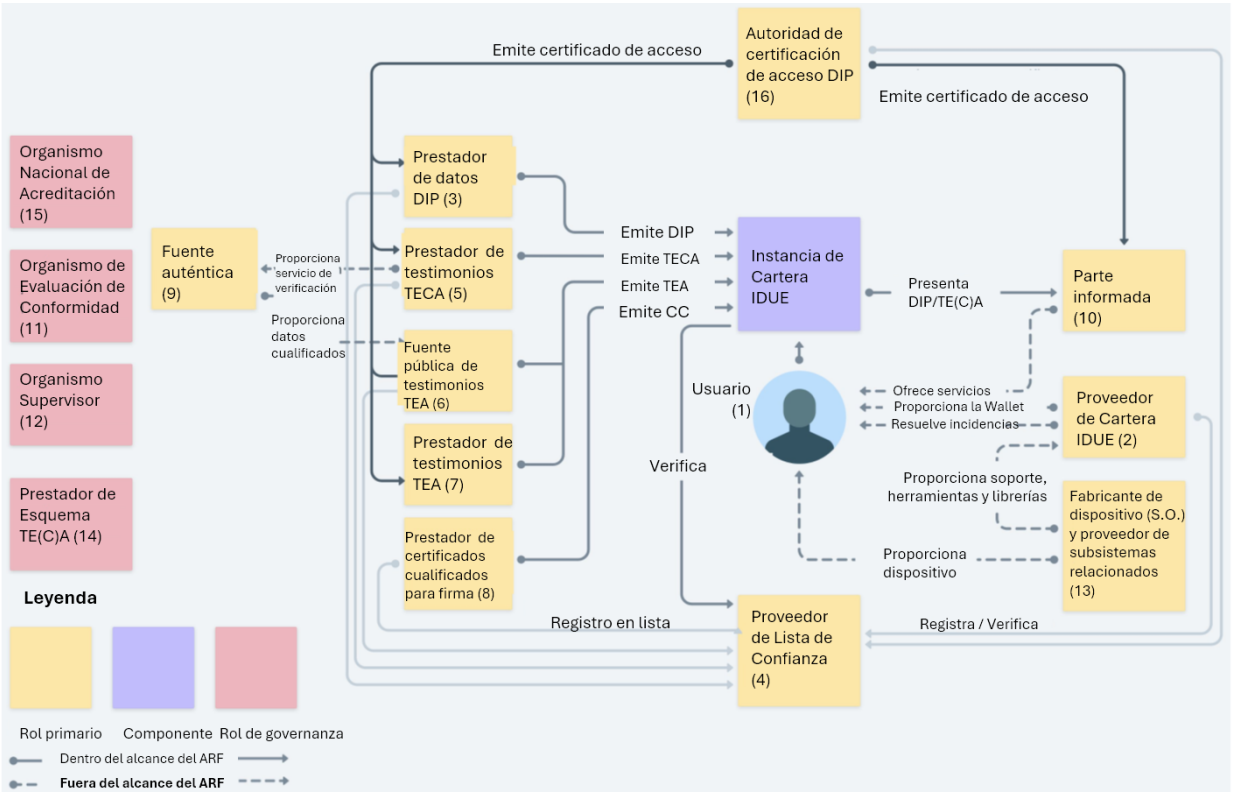

Figura 1: Visión general de las funciones del ecosistema Cartera IDUE

1. Usuarios de Unidades Cartera, véase el apartado 3.2,
2. Prestadores de Cartera, véase el apartado 3.3,
3. Prestadores de Datos de identificación Personal (DIP), véase el apartado 3.4,
4. Prestadores de confianza, véase el apartado 3.5,
5. Prestadores de Declaración Electrónica Cualificada de Atributos (DECA), véase la sección 3.6,
6. Declaración Electrónica de Atributos emitida por o en nombre de un organismo del sector público responsable de una fuente auténtica (DEA-AAPP) Prestadores, véase la sección 3.7,
7. Prestadores de Declaración Electrónica de Atributos (DEA), véase la sección 3.8,
8. Prestadores de Firma Electrónica Cualificada Remota, ver apartado 3.9,
9. Fuentes auténticas, véase el apartado 3.10,
10. Partes usuarias (informadas), véase el apartado 3.11,
11. Organismos de Evaluación de Conformidad OEC), véase el apartado 3.12,
12. Órganos de Vigilancia, véase el apartado 3.13,
13. Fabricantes de dispositivos y Prestadores de subsistemas relacionados, véase el punto 3.14,
14. Prestadores de Esquema de Atributos, ver Sección 3.15,
15. Organismos Nacionales de Acreditación, véase el apartado 3.16,

16. Acceda a las Autoridades de Certificación, consulte la Sección 3.17.

3.2 Usuarios de unidades Cartera

Los usuarios de Unidades Cartera utilizan la Unidad Cartera para recibir, almacenar y presentar DIP, DEA, DEA-AAPP o DEA no cualificada a Partes usuarias (informadas). Los usuarios también pueden crear firmas y sellos electrónicos Cualificados (FEC) y crear y presentar seudónimos.

El CIR 2024/2982 (entre otros) define "usuario de cartera" como "un usuario que está en control de la unidad de cartera". Estar en control de la Unidad Cartera implica poder presentar un DIP o declaración a una Parte usuaria (informada). En los casos de uso descritos en la versión actual del ARF, el usuario es el sujeto de los DIP de la unidad Cartera. El Usuario es también el sujeto de la mayoría de las declaraciones de la Unidad Cartera, pero puede haber declaraciones que no tengan sujeto, como los vales, o que se refieran a objetos poseídos o utilizados por el Usuario, como la tarjeta de matriculación de un vehículo.

Tenga en cuenta que este ARF asume que un dispositivo de Usuario es un dispositivo personal, lo que significa que el Usuario no lo compartirá con otras personas, y que sólo el Usuario puede acceder y controlar la Unidad Cartera.

Las próximas versiones del ARF pueden incluir casos de uso para la representación y la delegación, por ejemplo, un padre que representa a sus hijos o un director general que tiene derecho a firmar contratos en nombre de su empresa. Es concebible que estos casos de uso den lugar a situaciones en las que una unidad de Cartera posea los DIP de persona física de varias personas, o posea uno o más DIP de persona jurídica además de un DIP de persona física. No obstante, también son posibles otras soluciones. Los temas de la representación y la delegación se seguirán debatiendo con los Estados miembros en el futuro.

El uso de una Cartera de Identidad Digital Europea por los ciudadanos no es obligatorio en virtud del [Reglamento sobre la Identidad Digital Europea]. No obstante, cada Estado miembro proporcionará al menos una Cartera de Identidad Digital Europea en un plazo de 24 meses a partir de la entrada en vigor de los actos de ejecución contemplados en el [Reglamento sobre la Identidad Digital Europea].

3.3 Prestadores de Cartera

Los Prestadores de Carteras son los Estados miembros o las organizaciones autorizadas o reconocidas por los Estados miembros que ponen una Solución Cartera a disposición de los Usuarios. Todas las Soluciones Cartera deben estar certificadas tal y como se describe en el Capítulo 7.

Un Prestador de Carteras pone a disposición de un Usuario una combinación de varios productos y Servicios de Confianza, que le dan el control exclusivo sobre el uso de sus Datos de identificación Personal (DIP) y Declaraciones Electrónicas de Atributos (DECA, DEA-AAPP o DEA-AAPP), y cualquier otro dato personal dentro de su Unidad de Cartera. Esto también implica garantizar al Usuario el control exclusivo sobre el material criptográfico sensible (por ejemplo, claves privadas) relacionado con su Unidad Cartera.

Los Prestadores de Cartera son responsables de garantizar el cumplimiento de los requisitos de las Soluciones de Cartera.

Desde el punto de vista de los demás actores del ecosistema Cartera IDUE, el Prestador de Carteras es responsable de todos los componentes de la Unidad Cartera. Estos componentes se describen en la Sección 4.3.2. En particular, el Prestador de Carteras es responsable de garantizar que la Instancia de Cartera pueda acceder a un Dispositivo Criptográfico Seguro de Cartera (WSCD) que tenga un nivel de seguridad suficiente para garantizar que la Unidad de Cartera pueda alcanzar un Nivel de Aseguramiento "alto", tal y como exige el [Reglamento Europeo de Identidad Digital]. Esto es así incluso si el WSCD no es suministrado por el Prestador de Carteras sino que está integrado en el dispositivo del Usuario. Para más información, véase la sección 4.5. Otros agentes del ecosistema no necesitan interactuar con un de WSCD ni confiar explícitamente en él. Como se explica en la Sección 6.5.3, los Proveedores de Cartera proporcionan Declaraciones de Unidad de Cartera (WUA) a la Unidad de Cartera. El WUA certifica que la Unidad Cartera y todos sus componentes, incluido el WSCD, cumplen los requisitos pertinentes.

3.4 Prestadores de Datos de identificación Personal (DIP)

Los Prestadores de DIP son entidades de confianza responsables de:

- verificar la identidad del Usuario de conformidad con los requisitos de LoA high,
- emitir un DIP a la Unidad Cartera, y
- poner a disposición de las Partes usuarias (informadas), de forma que se preserve la privacidad, información que permita verificar la validez del DIP.

Las condiciones de estos servicios son competencia de cada Estado miembro.

Los Prestadores de DIP pueden ser las mismas organizaciones que hoy expiden documentos oficiales de identidad, medios electrónicos de identificación, etc. Los Proveedores de DIP pueden ser las mismas organizaciones que los Proveedores de Carteras. En caso de que una organización actúe a la vez como Proveedor de DIP y Proveedor de Cartera, deberá cumplir todos los requisitos aplicables tanto a los Proveedores de DIP como a los Proveedores de Cartera.

3.5 Prestador de listas de confianza

Un Proveedor de Listas de Confianza (TLP) es un organismo responsable de mantener, gestionar y publicar una Lista de Confianza. De conformidad con el artículo 22 del [Reglamento Europeo de Identidad Digital], un Prestador de Listas de Confianza es designado por un Estado miembro y notificado a la Comisión. Dentro del ecosistema de Cartera IDUE, existen listas de confianza para las siguientes entidades:

- Prestadores de Cartera,
- Prestadores de DIP,
- Prestadores de DECA,
- Prestadores de DEA-AAPP,

- Acceda a las autoridades de certificación,
- Prestadores de Firma Electrónica Cualificada Remota (QESRC).

Nota: También pueden existir Listas de Confianza y Prestadores de Listas de Confianza para Prestadores de la DEA no cualificados, pero esto queda fuera del ámbito del ARF.

Estas listas de confianza se describen con más detalle en las secciones 6.2.2, 6.3.2 y 6.4.2. Algunas listas de confianza contienen las anclas de confianza de las entidades pertinentes. Un anclaje de confianza es una combinación de una clave pública y el identificador de la entidad asociada y puede utilizarse para verificar las firmas creadas por dicha entidad.

La condición de entidad de confianza de una entidad puede verificarse comprobando si está presente en la lista de confianza correspondiente. Los Prestadores de Listas de Confianza ofrecen un servicio de inscripción para las entidades pertinentes. Corresponde a cada Prestador de Listas de Confianza determinar los términos y condiciones para que las entidades se registren, de conformidad con el artículo 22 del [Reglamento Europeo de Identidad Digital]. Para más información, consulte el 27 Tema el Tema 31.y

3.6 Prestadores de Declaración Electrónica Cualificada de Atributos (DECA)

Las DEA cualificadas son proporcionadas por Prestadores Cualificados de Servicios de Confianza (QTSP). El marco general de confianza para los QTSP (véase el capítulo III, sección 3 del [Reglamento Europeo de Identidad Digital] se aplica también a los Prestadores de DECA, pero también pueden definirse normas específicas para el Servicio de Confianza de emisión de DECA.

Los Prestadores de DECA mantienen una interfaz con las Unidades Cartera para proporcionar DECA previa solicitud. Potencialmente, también mantienen una interfaz con las Fuentes Auténticas para verificar los atributos, como se especifica en el Tema 42.

Es probable que, para la mayoría de los DECA, un Prestador de DECA necesite verificar la identidad de un Usuario al emitir un DECA. Corresponde a cada Prestador de DECA aplicar los procesos de autenticación de Usuarios necesarios, de conformidad con toda la legislación nacional y de la Unión aplicable. Tenga en cuenta que, cuando sea necesaria la verificación de la identidad del usuario, es probable que el usuario que solicita una DECA ya posea un DIP. Esto permitiría al Prestador de DECA llevar a cabo la identificación y autenticación del Usuario en LoA alto, solicitando y verificando los atributos del Usuario a partir del DIP en la Unidad Cartera.

Corresponde a cada Prestador de DECA determinar los términos y condiciones de estos servicios, más allá de lo especificado en el [Reglamento Europeo de Identidad Digital].

3.7 DEA emitida por o en nombre de un organismo del sector público responsable de una fuente auténtica (DEA-AAPP) Prestadores

Tal y como se especifica en el [Reglamento Europeo de Identidad Digital], una declaración puede ser emitida por o en nombre de un organismo del sector público responsable de una Fuente Auténtica. Este ARF

denomina a dicha declaración DEA-AAPP. Para una descripción de las Fuentes Auténticas, véase la Sección 3.10. Un organismo del sector público es principalmente una autoridad estatal, regional o local, o un organismo de derecho público.

Un Prestador de DEA-AAPP, es decir, un organismo del sector público que expide DEA-AAPP, no es un QTSP. Sin embargo, un Prestador de DEA-AAPP dispone de un certificado cualificado, expedido por un , que le permite firmar PuB- DEA. Una Parte usuaria (informada) verifica un DEA-AAPP verificando en primer lugar la firma sobre el DEA-AAPP, y posteriormente verificando la firma del certificado cualificado del Prestador de DEA-AAPP. Para más detalles, consulte la sección 6.6.3.6. El [Reglamento Europeo de Identidad Digital] estipula que los PuB-EAA, al igual que los DECA, tienen el mismo efecto legal que las declaraciones en papel. Corresponde a los Estados miembros definir los términos y condiciones para el suministro de DEA-AAPP, pero los DEA-AAPP

Los Prestadores cumplirán las mismas especificaciones técnicas y normas que los Prestadores de DIP y otras declaraciones.

Para conocer las definiciones y obligaciones precisas y jurídicamente vinculantes relativas a la emisión de DEA-AAPP, consulte el [Reglamento Europeo de Identidad Digital].

3.8 Prestadores no cualificados de Declaración Electrónica de Atributos (DEA)

Las DEA no cualificadas pueden ser suministradas por cualquier Prestador de Servicios de Confianza (no cualificado). Aunque estarán supervisadas por el [Reglamento Europeo de Identidad Digital], cabe suponer que otros marcos jurídicos o contractuales regirán en su mayor parte las normas de suministro, uso y reconocimiento de las DEA. Esos otros marcos pueden abarcar ámbitos políticos como las credenciales educativas o los pagos digitales, aunque también pueden basarse en los Prestadores de Declaraciones Electrónicas Cualificadas de Atributos. Para poder utilizar las DEA no cualificadas, los Prestadores de DEA ofrecen a los Usuarios una forma de solicitar y obtener dichas DEA. Esto implica que estos Proveedores de DEA no cualificados cumplen las especificaciones de la interfaz de la Unidad Cartera. Las condiciones de emisión de las DEA y los servicios conexos están sujetos a normas sectoriales.

3.9 Prestadores de Firma Electrónica Cualificada Remota (QESRC)

La Unidad Cartera permitirá al Usuario crear firmas electrónicas cualificadas o sellos sobre cualquier dato. Esto también mejorará el uso de la Unidad Cartera para firmar, de una forma natural y cómoda. La creación de una Firma Electrónica Cualificada o Sello mediante la Unidad Cartera puede realizarse de varias formas:

- la propia unidad Cartera podría certificarse como dispositivo cualificado de creación de firma o sello (QSCD), o bien
- la Unidad Cartera podría implementar la autenticación segura en una capacidad de invocación de firma electrónica o sello electrónico, como parte de un QSCD local o de un QSCD remoto gestionado por un QTSP.

Como parte del ecosistema, el uso de interfaces y protocolos comunes para el suministro de firmas y sellos electrónicos cualificados creará un mercado europeo unificado para los QTSP que ofrezcan servicios de firma a distancia. Los ciudadanos europeos podrán elegir cualquier , sin preocuparse por la interoperabilidad técnica, lo que fomentará la competencia.

Además de los prestadores de servicios de firma y sello electrónicos cualificados, también pueden existir prestadores de servicios de firma o sello electrónicos no cualificados. No obstante, estos proveedores quedan fuera del ámbito de aplicación del presente ARF.

3.10 Fuentes auténticas

Las Fuentes Auténticas son repositorios o sistemas públicos o privados, reconocidos o exigidos por ley, que contienen atributos sobre personas físicas o jurídicas. Las Fuentes Auténticas son fuentes de atributos sobre, por ejemplo, dirección, edad, sexo, estado civil, composición familiar, nacionalidad, títulos y licencias de educación y formación, títulos y licencias de cualificaciones profesionales, permisos y licencias públicas, o datos financieros y empresariales.

Las Fuentes Auténticas deben proporcionar una interfaz a los Prestadores de DECA para verificar la autenticidad de los atributos mencionados, ya sea directamente o a través de intermediarios designados reconocidos a nivel nacional. Las Fuentes Auténticas pueden actuar como Prestadores DEA-AAPP si cumplen los requisitos del Reglamento [Europeo de Identidad Digital], véase la Sección 3.7. En la figura 1 esto se indica con la flecha "proporciona datos cualificados".

3.11 Partes usuarias (informadas) e intermediarios

Las Partes usuarias (informadas) son personas físicas o jurídicas que confían en un sistema de identificación electrónica o en un Servicio de confianza. Solicitan atributos contenidos en un DIP, DEA, DEB-AAPP o DEA-AAPP a la Unidad Cartera, previa aprobación del Usuario y dentro de los límites de la legislación y las normas aplicables.

El motivo para confiar en la Unidad Cartera puede ser un requisito legal, un acuerdo contractual o su propia decisión. En particular, el [Reglamento Europeo de Identidad Digital] exige que los proveedores de plataformas en línea muy grandes acepten la Cartera IDUE para sus procesos de autenticación de usuarios.

Las Partes usuarias mantienen una interfaz con las Unidades Cartera para solicitar DIP y declaraciones, utilizando la autenticación de la Parte usuaria, tal y como se describe en la Sección 6.6.3.2. Si una Unidad Cartera presenta atributos de un DIP o declaración a una Parte usuaria, ésta podrá verificar la autenticidad de dichos atributos.

Para confiar en las Unidades Cartera con el fin de prestar un servicio, las Partes usuarias informan al Estado miembro en el que están establecidas de su intención de hacerlo, y registran el

que pretenden solicitar. Consulte la Sección 6.4.2 para obtener más información sobre el registro de Parte usuaria (informada). Durante una transacción, una Unidad Cartera verificará que la Parte usuaria (informada)

sólo solicita los atributos que ha registrado. En caso contrario, advertirá al usuario. Esto se explica en la sección 6.6.3.3.

Además, un Prestador de servicios de certificación puede incluir una política de divulgación en una declaración. política indica a qué Partes usuarias (informadas) debe (o no) presentar una Unidad de Cartera atributos específicos de esa declaración. Durante una transacción, la Unidad Cartera evalúa la basándose en los datos proporcionados por la Parte usuaria y advierte al usuario si el resultado de la evaluación es negativo. Para más información, consulte la sección 6.6.3.4.

Los denominados intermediarios constituyen una clase especial de Parte usuaria (informada). El artículo 5b (10) del [Reglamento Europeo de Identidad Digital] establece que "Los intermediarios que actúen en nombre de partes usuarias se considerarán partes usuarias y no almacenarán datos sobre el contenido de la transacción". Dicho intermediario es una parte que ofrece servicios a las Partes usuarias para, en su nombre, conectarse a las Unidades Cartera y solicitar los atributos de usuario que dichas Partes usuarias necesitan. A continuación, el intermediario envía los atributos presentados a la Parte usuaria "final". Esto implica que un intermediario realiza todas las tareas asignadas a una Parte usuaria en este ARF en nombre de la Parte usuaria "final". En particular:

1. El intermediario se registra una vez como Parte usuaria (informada) y obtiene un certificado de acceso (véase el apartado 6.6.3.2) con su propio nombre e identificador de Parte usuaria (informada). Este certificado de acceso no difiere de un certificado de acceso expedido a una Parte usuaria "normal", ya que un intermediario es, de hecho, una Parte usuaria.
2. A continuación, el intermediario registrará por separado cada una de las Partes usuarias "finales" que utilicen sus servicios, incluido el registro de los atributos que la Parte usuaria "final" desee solicitar. El intermediario obtiene un certificado de registro (véase el apartado 6.6.3.3) que muestra el nombre de la Parte usuaria (informada) "final". El Registrador verifica, de la forma decidida por el Estado miembro, que la Parte usuaria "final" está efectivamente utilizando los servicios del intermediario. Si todo es correcto, el Registrador expedirá un certificado de registro que contendrá un atributo adicional en el que se indicará que la Parte usuaria "final" está utilizando los servicios del intermediario.
3. A petición de una Parte usuaria (informada) "final", el intermediario solicitará la presentación de atributos de las Unidades Cartera, utilizando uno o varios de los flujos descritos en el apartado 4.4. Para ello, el intermediario utilizará su propio certificado de acceso (punto 1. anterior) y el certificado de registro de la Parte usuaria "final" (punto 2. anterior).
4. Si una Unidad Cartera, durante una transacción, recibe un certificado de registro indicando que

   la Parte usuaria (informada) utiliza los servicios de un intermediario, verifica que el nombre y el identificador del intermediario en el certificado de registro son idénticos al nombre y al identificador en el certificado de acceso. Si esta verificación falla, la Unidad Cartera lo trata como un fallo de autenticación de la Parte usuaria (informada). Si esta verificación tiene éxito, la Unidad Cartera muestra al Usuario el nombre del intermediario cuando solicita la aprobación del Usuario para presentar los atributos solicitados.
5. Cuando una Unidad Cartera presenta un DIP o una declaración al intermediario, éste verifica la autenticidad del DIP o la declaración, su estado de revocación, la vinculación al dispositivo y la

vinculación al usuario, así como cualquier presentación combinada de atributos, si procede, si así lo ha acordado con la Parte usuaria. Además, el intermediario puede tener que verificar la autenticidad de la Unidad Cartera y su estado de revocación. (Tenga en cuenta que una Parte usuaria (informada) no está obligada a llevar a cabo todas estas verificaciones. Por lo tanto, el intermediario y cualquier Parte usuaria (informada) que utilice sus servicios deben acordar qué verificaciones llevará a cabo el intermediario).

6. Si estas comprobaciones tienen éxito, el intermediario envía los atributos de usuario que ha obtenido de la Unidad Cartera a la Parte usuaria (informada) "final". Debe existir una interfaz entre un intermediario y una Parte usuaria, a través de la cual la Parte usuaria "final" pueda solicitar al intermediario que pida algunos atributos de usuario a una Unidad Cartera y que el intermediario utilice para devolver los valores de los atributos presentados por la Unidad Cartera. Sin embargo, especificar esta interfaz o los requisitos (de seguridad) que debe cumplir queda fuera del ámbito del ARF. En particular, no es necesario que los atributos de usuario estén cifrados de extremo a extremo entre la Unidad Cartera y la Parte usuaria "final", de forma que un intermediario no pueda verlos.
7. El intermediario eliminará cualquier DIP, declaración o WUA que haya obtenido de la Unidad Cartera, incluidos los atributos de usuario, inmediatamente después de enviar los atributos de usuario a la Parte usuaria (informada). Si el intermediario no envía ningún atributo de usuario a la Parte usuaria, por ejemplo porque ha fallado una de las comprobaciones del paso anterior, borrará los DIP, declaraciones o WUA inmediatamente después de haber completado todas las comprobaciones necesarias.

Obsérvese que este planteamiento implica que un intermediario (si sólo actúa como intermediario y nunca como Parte usuaria "final" por derecho propio) no necesitará un certificado de registro. Por el contrario, una Parte usuaria "final" que utilice los servicios de un intermediario no necesitará un certificado de acceso.

Como se explica en la sección 6.6.3.5, durante una transacción, una Unidad Cartera solicita al Usuario su aprobación para presentar cualquier atributo de usuario a la Parte usuaria (informada). En este proceso, la Unidad Cartera informa al Usuario de la identidad autenticada del intermediario (a partir del certificado de acceso), y también de la identidad de la Parte usuaria "final" y del hecho de que esta Parte usuaria está utilizando los servicios del intermediario (a partir del certificado de registro).

Para los requisitos de alto nivel sobre este tema, véase el Tema 52.

3.12 Organismos de Evaluación de Conformidad (OEC)

Los Organismos de Evaluación de Conformidad (OEC) son organismos públicos o privados acreditados por un organismo nacional de acreditación, que a su vez es designado por los Estados miembros de conformidad con el Reglamento 765/2008, artículo 6 quater (3). En particular, los OEC están acreditados para llevar a cabo evaluaciones en las que se basarán los Estados miembros antes de expedir una solución de Cartera o conceder el estatus de "cualificado" a un Prestador de Servicios de Confianza.

Las soluciones de Cartera serán certificadas por los CAB. Los CAB auditarán periódicamente a los QTSP.

En el capítulo 7 .se analizan las normas y esquemas utilizados por los CAB para cumplir sus tareas de certificación de las soluciones Cartera

3.13 Organismos de supervisión

Los Órganos de Supervisión revisan el correcto funcionamiento de los Prestadores de Cartera y otros actores del ecosistema de Carteras IDUE. Los órganos de supervisión serán creados y nombrados por los Estados miembros. Los Órganos de Supervisión serán notificados a la Comisión por los Estados miembros.

3.14 Fabricantes de dispositivos y proveedores de subsistemas relacionados

En el ecosistema Cartera IDUE, los agentes comerciales, como los fabricantes de dispositivos y los proveedores de subsistemas relacionados, desempeñan un papel importante para que una unidad Cartera funcione sin problemas y de forma segura. Los fabricantes de dispositivos y los proveedores de subsistemas relacionados proporcionan una plataforma sobre la que puede construirse una Unidad Cartera. Los Prestadores de Cartera se aseguran de que sus Unidades de Cartera utilicen esa para garantizar la facilidad de uso, la seguridad, la estabilidad y la conectividad. Los componentes proporcionados por los fabricantes de dispositivos y los proveedores de subsistemas relacionados pueden incluir, entre otros, hardware, sistemas operativos, hardware criptográfico seguro, bibliotecas y tiendas de aplicaciones.

3.15 Prestadores de Esquema de Atributos para DECA, DEB-AAPP y DEA

Los Prestadores de Esquemas de Atributos publican esquemas de atributos que describen la estructura de los QEAA, DEA-AAPP y DEA-AAPP, incluidos el identificador, la semántica y la codificación de todos los atributos. Estos esquemas de atributos se publican en Directrices de elaboración de declaraciones, véase la sección 5.5. Para los DIP y los mDL, la Comisión publica las Directrices de elaboración aplicables.

Un catálogo de las Directrices de elaboración de declaraciones publicadas permitirá a otras entidades, como las partes de confianza, descubrir qué declaraciones existen en el ecosistema de la Cartera IDUE y cómo pueden solicitarse y validarse los atributos de dichas declaraciones. La Comisión establece las especificaciones técnicas, normas y procedimientos para este fin. Los esquemas comunes, incluidos los de las organizaciones sectoriales, son fundamentales para la adopción generalizada de las declaraciones.

3.16 Organismos Nacionales de Acreditación

Los Organismos Nacionales de Acreditación ONA), en virtud del Reglamento (CE) nº 765/2008, son los organismos de los Estados miembros que realizan la acreditación con autoridad derivada del Estado miembro. Los NAB acreditan a los CAB (Sección 3.12) como organismos de certificación profesional competentes, independientes y supervisados, encargados de certificar las Soluciones Cartera frente a documento(s) normativo(s) que establece(n) los requisitos pertinentes. Las NAB supervisan los OEC a los que han expedido un certificado de acreditación.

3.17 Acceso a autoridades de certificación

Las Autoridades de Certificación de Acceso emiten certificados de acceso a todos los Prestadores de DIP, Prestadores de DECA, Prestadores de DECA no cualificados y Partes usuarias del ecosistema de Carteras IDUE. Cuando estas entidades interactúan con una Unidad Cartera para emitir o solicitar un DIP o una declaración, presentarán un certificado de acceso para demostrar su autenticidad y validez.

Las autoridades de certificación de acceso deben ser notificadas por un Estado miembro a la Comisión. Como parte del proceso de notificación, los anclajes de confianza de la autoridad de certificación de acceso deben incluirse en una lista de confianza. Un anclaje de confianza es la combinación de una clave pública y un identificador de la entidad asociada. Las Unidades Cartera necesitan estas anclas de confianza para verificar las firmas sobre los certificados de acceso que se les presentan cuando se emite un nuevo DIP o declaración o cuando reciben una solicitud de presentación de atributos de una Parte usuaria (informada).

4 Arquitectura de alto nivel

4.1 Introducción

Este capítulo proporciona una visión general de los componentes principales del ecosistema Cartera IDUE, sus interfaces y los principios generales de diseño. Este capítulo está estructurado de la siguiente manera:

- La sección 4.2 discute los principios de diseño que guiaron el diseño del ecosistema Cartera IDUE, tal y como se describe en este ARF.
- La sección 4.3 presenta una visión general de la arquitectura del ecosistema, centrándose en los componentes que conforman una Unidad Cartera y en las interfaces entre una Unidad Cartera y otras entidades, así como en los protocolos utilizados en estas interfaces.
- En la sección 4.4 se analizan los distintos flujos de presentación de declaraciones que permite esta arquitectura y, en particular, los mecanismos previstos para habilitar y proteger los flujos de presentación remotos en los que la Unidad Cartera y la Parte usuaria (informada) interactúan a través de Internet.
- La Sección 4.5 discute brevemente los diferentes tipos de arquitectura que un Prestador de Cartera puede utilizar para implementar uno o más Dispositivo(s) Criptográfico(s) Seguro(s) de Cartera en sus Soluciones de Cartera.
- La sección 4.6 presenta diagramas de estado para todas las entidades y componentes principales del ecosistema Cartera IDUE, analizando todos los estados en los que puede encontrarse un componente concreto, así como las condiciones que desencadenan las transiciones de estado. • En la sección 4.7 se analiza cómo se implementarán y utilizarán los seudónimos dentro de una Unidad Cartera.

4.2 Principios de diseño

Para traducir eficazmente el [Reglamento Europeo de Identidad Digital] en una arquitectura técnica fácil de usar, centrada en la privacidad y segura, es crucial establecer principios de diseño. Estos principios,

arraigados en el marco normativo y enriquecidos con las mejores prácticas del sector, servirán de directrices fundamentales. Este planteamiento garantiza el cumplimiento de los requisitos relativos al usuario, la privacidad, la seguridad y la interoperabilidad transfronteriza. Demuestra un compromiso tanto con la alineación normativa como con la excelencia en el diseño de la arquitectura de la Cartera IDUE.

4.2.1 Centrado en el usuario

El ecosistema de Cartera IDUE prioriza la centralidad del usuario como principio básico de diseño. Esto significa situar las necesidades y la experiencia del usuario al frente de cada decisión de diseño. La Unidad Cartera debe ser intuitiva y fácil de usar, con una integración perfecta en los casos de uso existentes. Los usuarios deben tener pleno control sobre sus atributos y privacidad, con información transparente sobre qué atributos se presentan y a quién. Además, la Unidad Cartera debe ser accesible e inclusiva, para usuarios con diferentes conocimientos técnicos y capacidades. Al dar prioridad al usuario, el ecosistema Cartera IDUE fomenta la confianza y favorece la adopción generalizada, logrando en última instancia su objetivo de proporcionar a los usuarios una gestión de identidad digital segura y cómoda.

4.2.2 Interoperabilidad

El ecosistema Cartera IDUE da prioridad a la interoperabilidad como principio básico de diseño. Esto garantiza que una unidad de Cartera funcione sin problemas a través de las fronteras dentro de la UE. Los usuarios pueden viajar libremente y utilizar con confianza sus carteras de identidad digital para diversos servicios, desde plataformas de administración electrónica hasta interacciones privadas en línea. La interoperabilidad fomenta el intercambio seguro de datos mediante protocolos normalizados, lo que permite a las entidades de confianza verificar las credenciales sin esfuerzo. Esto no sólo simplifica la experiencia del usuario, sino que refuerza la seguridad general del sistema. Además, la interoperabilidad evita la fragmentación del mercado al crear equitativas para las distintas soluciones de Cartera. Fomenta la competencia y la colaboración, impulsando en última instancia la innovación en el ecosistema de Carteras IDUE. Al dar prioridad a la interoperabilidad, la arquitectura de Cartera IDUE sienta las bases de un ecosistema de Cartera IDUE fiable y universalmente aceptado en toda la UE.

4.2.3 Privacidad desde el diseño

La arquitectura de Cartera IDUE incorpora el principio de privacidad por diseño. Esto significa que la protección de los datos de los usuarios es un pilar fundamental del diseño de la arquitectura. El principio de minimización de datos guía la recogida de información personal, garantizando que las Partes usuarias (informadas) recojan únicamente los atributos que necesitan y para los que se han registrado. Al permitir la divulgación selectiva de atributos, la Unidad Cartera otorga a los usuarios un control granular sobre qué datos se presentan y a quién. La transparencia está integrada en el sistema, con explicaciones claras sobre cómo se utilizan y protegen los datos. Al hacer de la privacidad una piedra angular desde el , el ecosistema Cartera IDUE pretende fomentar la confianza y proteger los derechos fundamentales de sus usuarios. Por último, se toman medidas para evitar que los Usuarios sean rastreados por Partes usuarias (informadas), Prestadores de DIP o Prestadores de declaraciones.

Para más información, consulte los apartados 7.4.3.4 y 7.4.3.5.

4.2.4 Seguridad desde el diseño

La arquitectura de Cartera IDUE adopta el principio de seguridad por diseño. Esto significa que las consideraciones de seguridad se entretejen en el tejido mismo del diseño de la arquitectura. A lo largo del proceso de diseño, se identifican y mitigan las vulnerabilidades potenciales. Las prácticas de codificación segura son obligatorias, y la propia arquitectura minimiza las superficies de ataque compartimentando los datos sensibles y los controles de acceso. Al dar prioridad a la seguridad desde el principio, la arquitectura de Cartera IDUE pretende ser intrínsecamente resistente a los ciberataques y a las violaciones de datos, fomentando la confianza de los usuarios en este ecosistema de Cartera IDUE.

Para más información, consulte los apartados 7.4.3.2 y 7.4.3.3.

4.3 Arquitectura de referencia

4.3.1 Visión general

La figura siguiente ofrece una visión general de la arquitectura del ecosistema Cartera IDUE y sus componentes. En comparación con la Figura 1, esta figura presenta más detalles sobre la composición de una Unidad Cartera y sus interfaces con otras entidades. Los componentes representados de una Unidad Cartera se describen en la sección 4.sección 4.3.3. 3.2, mientras que las interfaces se describen en la Las demás entidades que aparecen en la figura ya se describieron en el Capítulo 3.

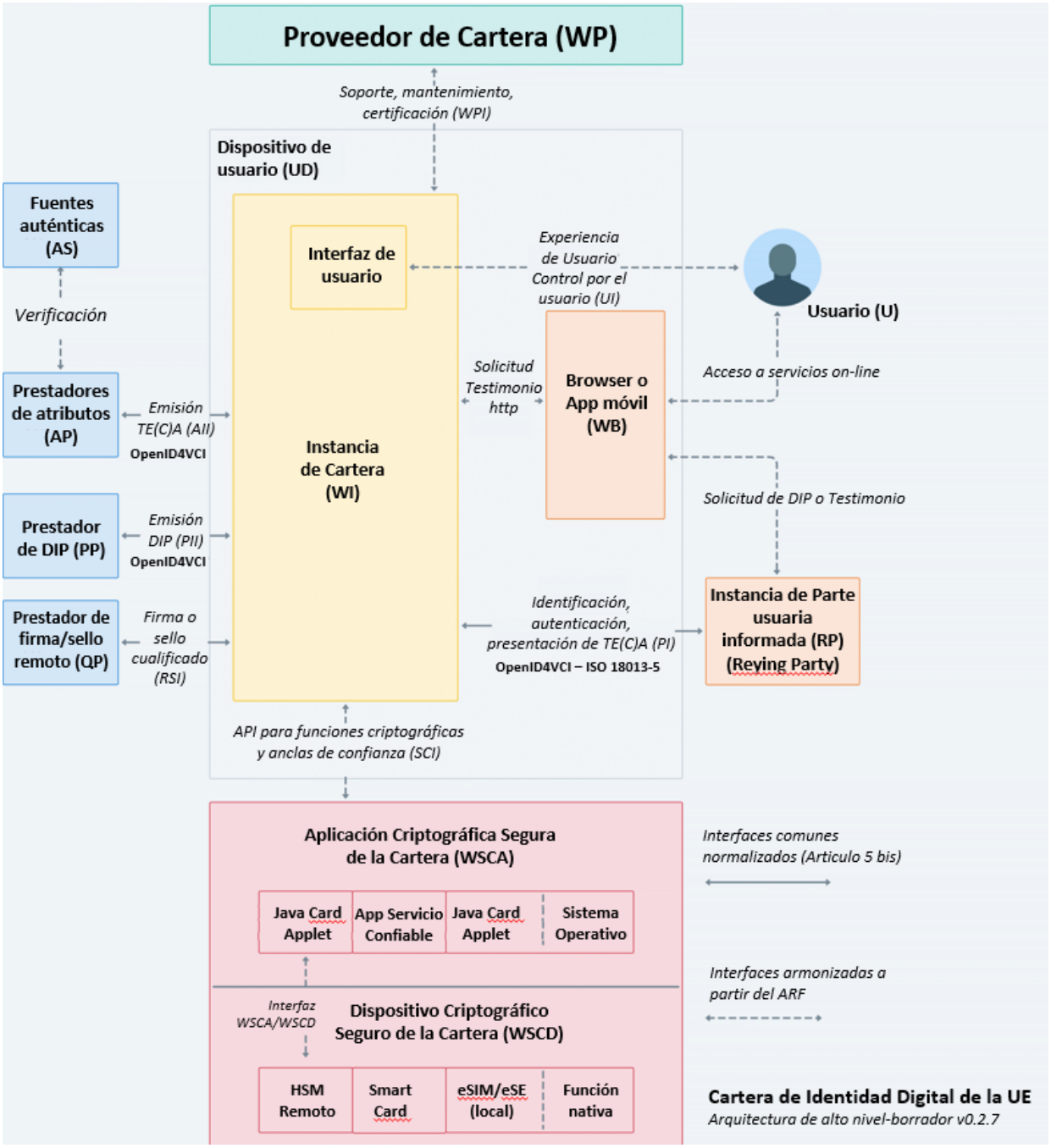

Figura 2: Arquitectura de referencia del ecosistema Cartera IDUE

Tenga en cuenta que un dispositivo de Usuario puede alojar más de una Unidad Cartera, ya sea proporcionada por varios Proveedores de Carteras o por el , si ese Proveedor de Carteras lo admite. Si un dispositivo de usuario aloja más de unidad Cartera, todas las afirmaciones de este ARF relativas a una unidad Cartera y sus componentes

para cada Unidad Cartera de forma independiente.

4.3.2 Componentes de una unidad Cartera

Se han identificado los siguientes componentes básicos de una Unidad Cartera:

- **Dispositivo de Usuario (UD)**: Un Dispositivo de Usuario comprende el hardware, el sistema operativo y el entorno de software necesarios para alojar y ejecutar la Instancia de Cartera. Los requisitos mínimos de hardware y software para el dispositivo de usuario serán determinados por el Prestador de Carteras.
- **Instancia de Cartera (WI)**: La app o aplicación instalada en un dispositivo de Usuario, que es una instancia de una Solución Cartera y pertenece y es controlada por un Usuario. Este componente implementa la lógica de negocio central y las interfaces como se muestra en la Figura 2. Interactúa directamente con WSCA/WSCD (WSCA/WSCD). Interactúa directamente con la WSCA/WSCD (véanse las viñetas a continuación) para gestionar de forma segura los activos criptográficos y ejecutar funciones criptográficas, garantizando un alto nivel de seguridad para la autenticación.
- **Dispositivo Criptográfico** Seguro de Cartera **(WSCD):** dispositivo resistente a la manipulación que proporciona un entorno vinculado a la aplicación criptográfica segura de cartera y utilizado por ésta para proteger activos críticos y ejecutar funciones criptográficas de forma segura. Esto incluye un almacén de claves, pero también el entorno en el que se ejecutan las funciones críticas para la seguridad. El WSCD es a prueba de manipulación y duplicación. Un WSCD puede formar parte de varias unidades Cartera, por ejemplo en el caso de un HSM remoto. El WSCD consta de dos partes: el hardware del WSCD incluye el hardware emitido por el proveedor del WSCD y el firmware del WSCD incluye el software relacionado con la seguridad, como el sistema operativo y las bibliotecas criptográficas proporcionadas por el proveedor del WSCD. La figura 2 muestra cuatro posibles arquitecturas de seguridad diferentes para el WSCD (para más detalles, véase la sección 4.5):
  - un WSCD remoto, un dispositivo remoto, como un módulo de seguridad de hardware (HSM), al que se accede a través de una red.
  - un WSCD externo local, un dispositivo externo, como una tarjeta inteligente emitida al Usuario específicamente para este fin,
  - un WSCD interno local, un componente dentro del dispositivo de usuario, como una SIM, una e-SIM o un elemento seguro integrado,
  - un WSCD nativo local, un componente integrado en el dispositivo del usuario al que se accede a través de una API proporcionada por el sistema operativo.
- **Aplicación Criptográfica Segura de Cartera (WSCA):** una aplicación que gestiona los datos críticos. activos al estar vinculado y utilizar las funciones criptográficas y no criptográficas proporcionadas por el Dispositivo Criptográfico Seguro de Cartera. La WSCA interactúa directamente con la Instancia Cartera. Para más detalles, véase la sección 4.5.
- **Prestador de Carteras (WPB**): El Proveedor de Carteras ofrece a los Usuarios asistencia con sus Unidades de Cartera, realiza el mantenimiento esencial y emite Declaraciones de Unidad de Cartera a través de la Interfaz de Proveedor de Cartera (WPI).

4.3.3 Interfaces y protocolos de la Unidad Cartera

La Figura 2 muestra las siguientes interfaces entre los componentes de Unidad Cartera, o entre la Unidad Cartera y otras entidades del ecosistema Cartera IDUE:

- La **Interfaz de Proveedor de Cartera (WPI)** es utilizada por la Instancia de Cartera para comunicarse con el Proveedor de Cartera para solicitar y emitir la Declaración de Unidad de Cartera, así como para proporcionar apoyo al Usuario y recopilar información agregada y consentida por el usuario de una manera que preserve la privacidad para suministrar la Unidad de Cartera, de conformidad con la legislación aplicable. Dado que el Prestador de Carteras es responsable de ambos lados de esta interfaz, no se normalizará en el ámbito del ecosistema de Carteras IDUE.

- La **Interfaz de Usuario IU)** es el punto de interacción y comunicación entre el Usuario y la Instancia Cartera. Esta interfaz no se estandarizará en el ámbito del ecosistema Cartera IDUE.

- **La interfaz de presentación (PI)** permite a las instancias de la Parte usuaria (informada) solicitar y recibir DIP, DEA-AAPP, DEA-AAPP y DEA-AAPP de las unidades de la Cartera de forma segura. Esta interfaz admite interacciones remotas y de proximidad. Para los flujos de presentación remotos, como se detalla en la Sección 4.4.3, la Instancia Cartera implementa el protocolo OpenID for Verifiable Presentation [OpenID4VP] en combinación con la [W3C Digital Credentials API]. En cambio, para el flujo de presentación de proximidad, esta interfaz se adhiere a la norma [ISO/IEC 18013-5], véase el apartado 4.4.2. La misma interfaz también puede ser utilizada por otra Unidad Cartera para solicitar atributos de Usuario, ver Sección 6.6.4.

- **La Interfaz Criptográfica Segura (SCI)** permite a la Instancia Cartera comunicarse con la Aplicación Criptográfica Segura Cartera (WSCA). Esta interfaz está diseñada específicamente para gestionar activos críticos y ejecutar funciones criptográficas. Para poder soportar diferentes tipos de WSCA/WSCD, las Instancias de Cartera pueden necesitar ser capaces de manejar múltiples sabores de esta interfaz.

- **La Interfaz de Emisión de DIP (PII)** cumple con el estándar [OpenID4VCI] y se utiliza cuando la Unidad Cartera se comunica con un Proveedor de DIP para solicitar y recibir DIP que se almacenarán dentro de la Unidad Cartera.

- **La Interfaz de Emisión de Declaraciones (AII)** cumple con el estándar [OpenID4VCI] y es utilizada por la Unidad Cartera para solicitar diversas declaraciones que el Usuario desea incluir en su Unidad Cartera.

- **La Interfaz de Firma** Electrónica Cualificada o Sello Remoto **(RSI)** facilita la comunicación entre la Unidad Cartera y un Prestador de Firma Electrónica Cualificada o Sello Remoto (QESRC). Esta interfaz es utilizada por la Unidad Cartera para generar una Firma Electrónica Cualificada o un Sello.

*Tenga en cuenta que la "Interfaz de solicitud de eliminación de atributos a la Parte usuaria (informada)" y la "Interfaz de notificación de la Parte usuaria (informada) a la DPA", que se mencionan en el Reglamento, no se representan como interfaces en la Figura 2. La funcionalidad que permite a un usuario solicitar a una Parte usuaria que elimine datos personales (es decir, atributos de usuario) obtenidos de la Unidad de Cartera

del se considera una característica de la Solución de Cartera. Lo mismo ocurre con las funciones que permiten al usuario denunciar a una Parte usuaria (informada) ante una Autoridad de Protección de Datos.

4.4 Flujos de presentación de datos

4.4.1 Visión general

En esta sección se definen cuatro flujos de comunicación distintos que pueden utilizarse cuando una Unidad Cartera presenta un DIP o una declaración a una Instancia Parte usuaria (informada):

- **Flujo Supervisado por Proximidad**: En este flujo, el Usuario y su Dispositivo de Usuario están físicamente cerca de la Instancia de la Parte que Confía. Los DIP y las declaraciones se intercambian utilizando tecnología de proximidad (por ejemplo, NFC, Bluetooth) entre la Unidad Cartera y la Instancia de la Parte usuaria (informada). Ambos dispositivos pueden estar con o sin conectividad a Internet. Un representante humano de la Parte usuaria (informada) supervisa el proceso.
- **Flujo no supervisado de proximidad**: Este flujo es como el supervisado, pero la Unidad Cartera presenta declaraciones a una máquina, sin supervisión humana. Las interfaces y protocolos utilizados en este flujo son los mismos que para el flujo supervisado de proximidad, y se describen en la sección 4.4.2.
- **Flujo remoto desde el mismo dispositivo**: En este flujo, el usuario utiliza un navegador web u otra aplicación en su dispositivo de usuario para acceder a un servicio de la Parte usuaria (informada). Si consume el

  requiere que la Parte usuaria obtenga atributos específicos de la Unidad Cartera del , la Parte usuaria envía una solicitud de presentación a la Unidad Cartera. Como se explica en la sección 4.4.3.2, esta solicitud es gestionada por el navegador web del dispositivo del usuario, utilizando una solución como la [W3C Digital Credentials API] y, entre bastidores, una API entre aplicaciones proporcionada por el sistema operativo del dispositivo.
- **Flujo remoto entre dispositivos**: En este flujo, el usuario utiliza un navegador web en un dispositivo distinto de su Instancia de Cartera, por ejemplo un ordenador de sobremesa o portátil, para acceder al servicio de la Parte usuaria (informada). Si la Parte usuaria (informada) necesita enviar una solicitud de presentación a la Instancia de Cartera del usuario, presenta esta solicitud al navegador web del otro dispositivo. De nuevo utilizando la [W3C Digital Credentials API], este navegador web podría establecer un canal de comunicación seguro entre el otro dispositivo y el dispositivo del Usuario. La sección 4.4.3.3 explica esto con más detalle.

Los casos de uso específicos integran uno o varios de estos . Cada uno de estos flujos se describe con más detalle en una de las secciones siguientes.

4.4.2 Flujos de presentación de proximidad

La figura 3 muestra cómo funciona la presentación de declaraciones cuando el usuario y su dispositivo de usuario se encuentran físicamente cerca de la instancia de la parte de confianza. En este , la norma [ISO/IEC 18013-5] especifica cómo se establece un canal de comunicación y cómo se intercambian una solicitud de presentación y la respuesta correspondiente.

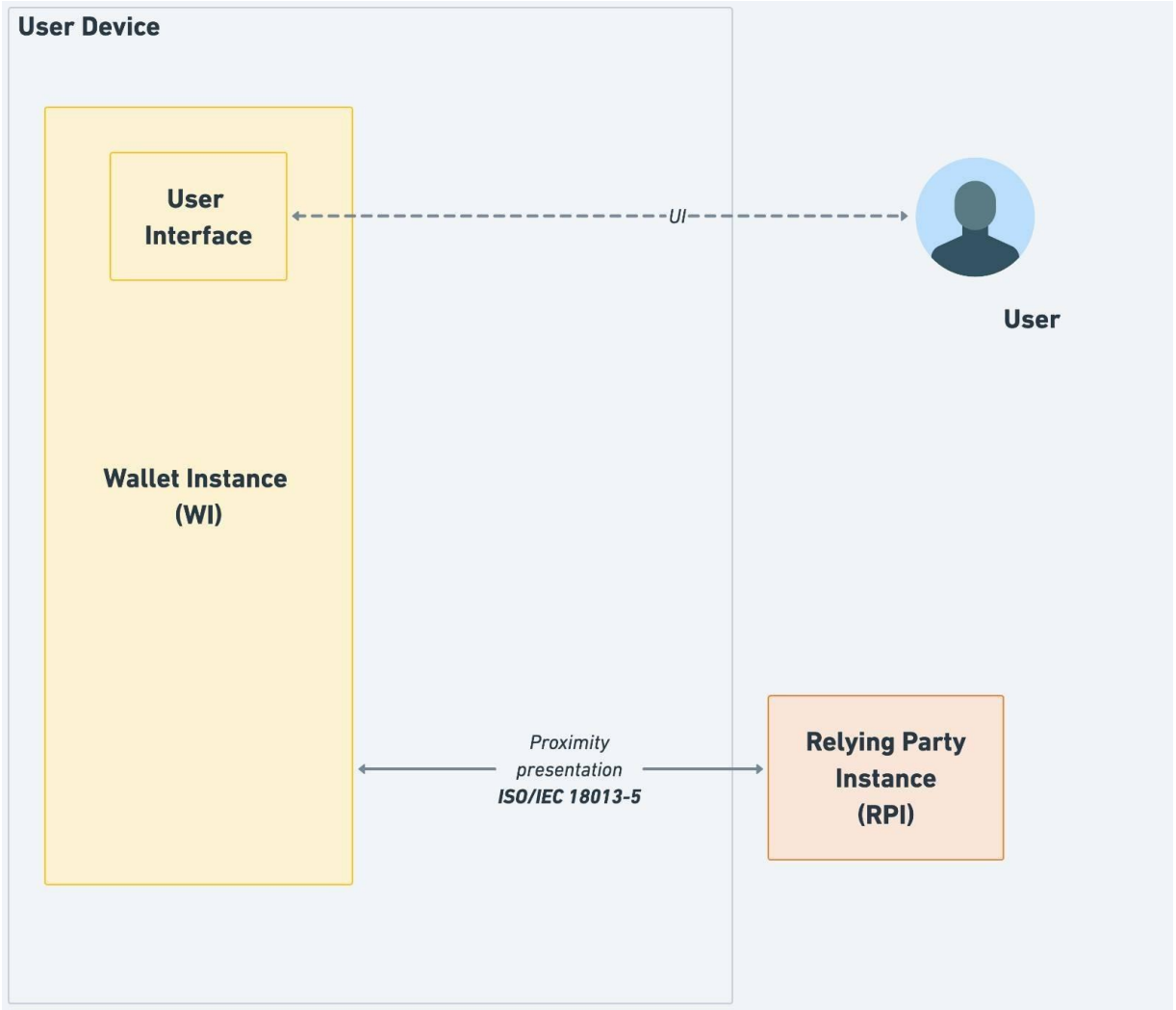

Figura 3: Presentaciones de proximidad

El flujo de presentación de atributos comienza cuando el Usuario abre la Instancia de Cartera y le indica que muestre un código QR o presente una etiqueta NFC. Este código QR o etiqueta NFC contiene la información necesaria para establecer una conexión NFC, BLE o Wi-Fi Aware. La Instancia de la Parte usuaria (informada) escanea el código QR o la etiqueta NFC y establece la conexión. El código QR o la etiqueta NFC también contiene la información necesaria para crear un canal seguro autenticado y cifrado entre ambas entidades.

4.4.3 Flujos de presentación a distancia

4.4.3.1 Introducción

Los flujos de transacciones remotas son casos de uso en los que la Instancia de la Parte usuaria está alejada del usuario y del dispositivo del usuario. La Instancia de la Parte usuaria solicita datos a la Unidad de Cartera a través de Internet, utilizando un navegador. Estos casos de uso pueden distinguirse a su vez como flujos del mismo dispositivo, en los que el navegador se ejecuta en el mismo dispositivo que la Unidad Cartera, y flujos entre dispositivos, en los que el navegador se encuentra en un dispositivo diferente.

Los flujos de presentación a distancia plantean una serie de retos que no están presentes en los flujos de proximidad:

1. **Flujos seguros entre dispositivos**: Los flujos entre dispositivos son vulnerables a los ataques de suplantación de identidad y retransmisión, por lo que es necesario reforzar las medidas de seguridad. Las comprobaciones de proximidad, gestionadas por el sistema operativo del dispositivo de usuario, pueden mitigar los riesgos derivados de estas vulnerabilidades aprovechando las funciones de seguridad integradas para verificar la autenticidad de las interacciones, garantizando que sean seguras y fiables.
2. **Selección de la Unidad Cartera**: En los flujos remotos, en los que las interacciones no se originan en Unidad Cartera, los Usuarios pueden encontrar dificultades a la hora de seleccionar la Unidad Cartera adecuada para satisfacer una solicitud de presentación específica, especialmente cuando hay varias Unidades Cartera presentes en el dispositivo. Una interfaz unificada proporcionada por el navegador web y el sistema operativo del dispositivo puede agilizar este proceso, ofreciendo una experiencia de usuario fluida e intuitiva.
3. **Mecanismo de invocación**: Establecer un canal de comunicación entre la Unidad Cartera y la Instancia de Parte usuaria (informada) remota presenta retos debido a la inconsistencia de los métodos de invocación. Un enfoque considerado por los organismos de normalización consiste en utilizar esquemas URI personalizados, como "mdoc://" u "openid4vp://". En este enfoque, el sistema operativo del dispositivo activaría la Unidad Cartera cuando la Instancia Parte usuaria (informada) solicitara una conexión a través de una URI personalizada. Otro enfoque es el uso de enlaces universales vinculados a dominios (también conocidos como enlaces de aplicaciones). Sin embargo, depender de esquemas URI personalizados o enlaces universales introduce variabilidad en las experiencias de los usuarios en diferentes navegadores y sistemas operativos, lo que resulta en ineficiencias operativas y riesgos potenciales de seguridad. Una interfaz proporcionada por el navegador web y el sistema operativo del dispositivo no necesita esquemas de URL personalizados ni enlaces universales para invocar una Unidad Cartera.
4. **Verificación clara del origen**: La protección contra ataques de retransmisión requiere una identificación precisa del origen de la Instancia de Parte usuaria (informada). Incluir la información de origen, como el dominio del sitio web o el nombre del paquete de la aplicación, en la solicitud de presentación garantiza la autenticidad de la solicitud y aumenta la confianza tanto de las unidades Cartera como de los usuarios.

5. **Vinculación de la sesión**: Al presentar un DIP o una declaración a una Parte usuaria (informada) remota, los usuarios tienen que cambiar de contexto. Los protocolos existentes pueden permitir ataques en los que el

   los contextos no están vinculados entre sí, lo que da lugar al secuestro de sesiones. El uso de una interfaz proporcionada por el navegador web y el sistema operativo del dispositivo permite incluir información sobre una sesión en una solicitud de presentación. Al mismo tiempo, el navegador y el sistema operativo gestionan adecuadamente el cambio de contexto, evitando el secuestro de sesión.

En las siguientes secciones se describe cómo se podrían resolver estos problemas para los flujos de presentación remota en el mismo dispositivo y entre dispositivos, utilizando la [API de credenciales digitales del W3C]. Se espera que esta API establezca un comportamiento coherente del navegador para invocar Unidades Cartera, abordando estos retos. Cuando sea compatible con los navegadores, debería considerarse la opción preferida.

La versión actual de la [API de credenciales digitales del W3C] amplía la API de nivel 1 de gestión de credenciales (la misma API utilizada por WebAuthn / Passkeys, véase la sección 4.7) para permitir los sitios web soliciten una declaración. Esto se consigue proporcionando una secuencia de "solicitudes de presentación", donde cada solicitud de presentación incluye un "protocolo de intercambio" y "datos de solicitud". El formato de los datos de solicitud es específico del protocolo de intercambio. Las especificaciones de la API de credenciales digitales incluirán un registro de protocolos compatibles. Para obtener más información, consulte el documento de debate Tema F: API de credenciales digitales.

Sin embargo, la [API de credenciales digitales del W3C] aún está en desarrollo y todavía no se ha estandarizado. Para que la [API de credenciales digitales del W3C] sea obligatoria para este ARF en el futuro, tendrá que ajustarse a los principios y expectativas descritos en el capítulo 3 del documento de debate del tema F. Además, la API aún no se ha implementado en todos los navegadores y sistemas operativos. Además, la API aún no ha sido implementada por todos los navegadores y sistemas operativos.

Hasta que se cumplan estas tres condiciones (estandarización, cumplimiento de las expectativas y amplio apoyo), el uso de esta API por parte de las Unidades Cartera y Partes usuarias es opcional, y también pueden seguir utilizándose esquemas de URL personalizados. Si una Unidad Cartera implementa un esquema de URL personalizado, necesitará implementar mitigaciones para los retos descritos en esta sección.

4.4.3.2 Flujos de presentación remota en el mismo dispositivo

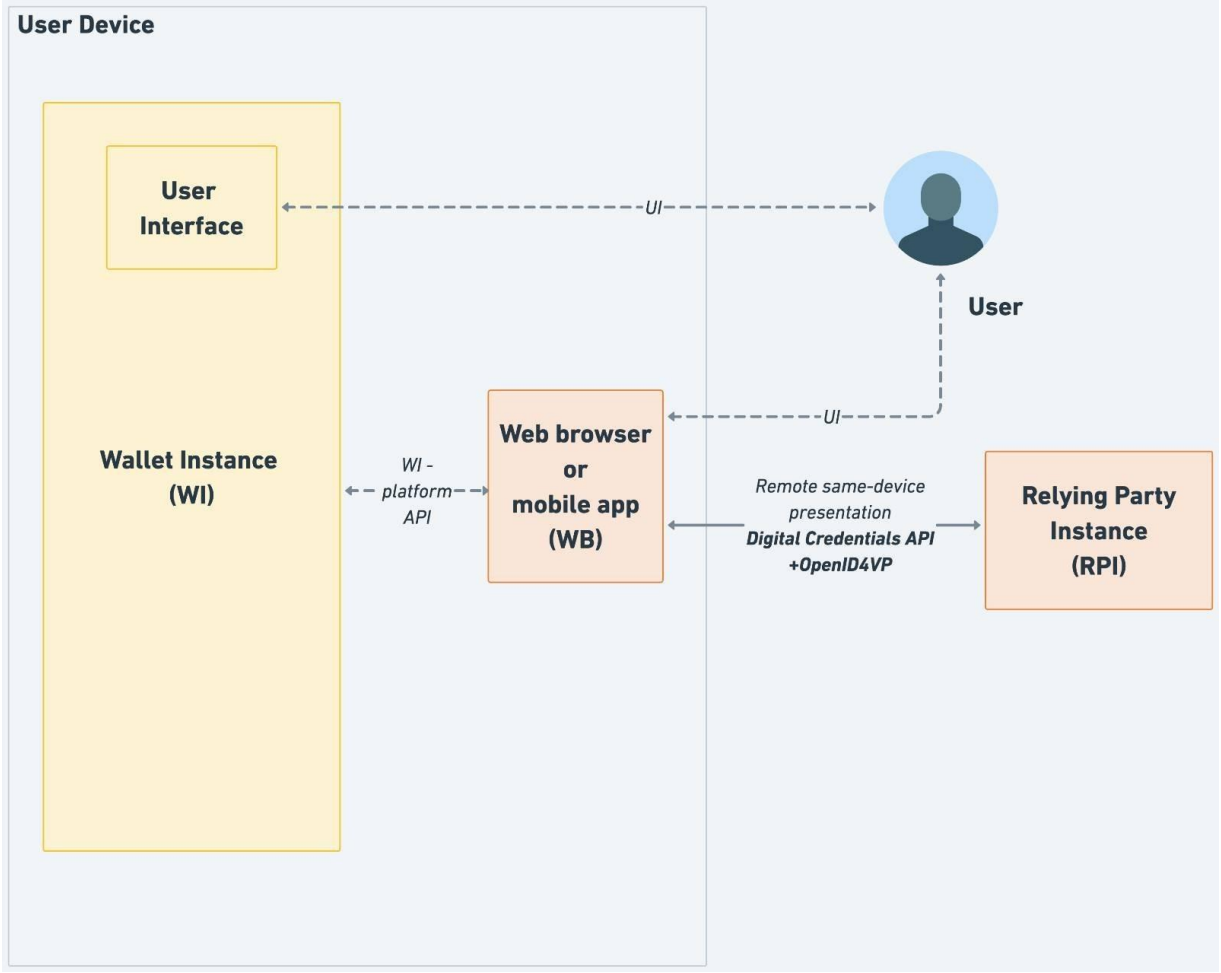

Figura 4: Presentaciones remotas del mismo dispositivo

En comparación con la Figura 2, la Figura 4 muestra detalles adicionales. En concreto, muestra el navegador del dispositivo del usuario y las interfaces relevantes de este navegador:

- La interfaz de **presentación remota del mismo dispositivo** establece la comunicación entre el navegador web y una Instancia de la Parte usuaria remota, que puede operar en un servidor gestionado por la Parte usuaria. Esta interfaz puede ajustarse a la [API de credenciales digitales], que es una API de navegador que se está normalizando actualmente en el W3C.
- La interfaz **WI-platform API** es una API entre aplicaciones que puede implementar el mecanismo Digital Cre- dentials API a nivel de sistema operativo. Sin embargo, actualmente no hay planes para estandarizar esta interfaz a nivel de las llamadas API. Estas llamadas se especificarán en la documentación para desarrolladores del sistema operativo correspondiente. Uno de los elementos clave de esta API es que la Unidad Cartera recibe información fiable sobre el origen de la solicitud de presentación.

Obviamente, el navegador también tiene una interfaz de usuario que permite al usuario interactuar con él. Este

no se normalizará en el contexto del ecosistema Cartera IDUE.

Un flujo remoto de presentación de atributos desde el mismo dispositivo comienza cuando el usuario accede al sitio web de la Parte usuaria (informada) utilizando un navegador en su dispositivo. El sitio web puede ofrecer al usuario la opción de presentar atributos desde su Unidad Cartera, normalmente a través de un botón o una interfaz similar. Cuando el usuario selecciona esta opción, el navegador le pide permiso para conectarse a la unidad Cartera. Una vez concedido el permiso, la Instancia de la Parte usuaria (informada) envía una solicitud de presentación conforme con la especificación OpenID4VP al navegador a través de la API de Credenciales Digitales. El navegador, trabajando en tándem con el sistema operativo (SO) del dispositivo, reenvía la solicitud a la Unidad Cartera utilizando la API WI-plataforma. Si el dispositivo aloja Unidades Cartera, el navegador y el SO determinarán qué Unidad Cartera debe gestionar la solicitud. Esta decisión puede implicar la consulta al usuario.

La Unidad Cartera seleccionada procesa la solicitud de presentación y solicita la aprobación del Usuario antes de devolver al los atributos solicitados en un formato cifrado. A continuación, el navegador reenvía esta respuesta cifrada a la Instancia de Parte usuaria (informada) remota.

La Figura 4 también ilustra un flujo de presentación de atributos entre aplicaciones. En este escenario, una aplicación en el dispositivo del usuario, como una aplicación bancaria o de compras, actúa como Instancia de Parte usuaria (informada), en lugar de un navegador web. La aplicación puede aprovechar los atributos de Usuario recuperados de la Unidad Cartera para varios propósitos, incluyendo la autenticación del Usuario o rellenar automáticamente campos de datos como el nombre y la dirección.

En este caso de uso, el flujo de presentación de atributos comienza cuando el usuario abre la aplicación e inicia una solicitud de atributos de la Unidad Cartera a través de la API de la plataforma WI. Cabe destacar que se trata de la misma API que se utiliza en el flujo de presentación remota en el mismo dispositivo en el que interviene un navegador. La principal diferencia radica en la información de origen incluida en la solicitud de presentación, que puede variar.

4.4.3.3 Flujos de presentación remota entre dispositivos

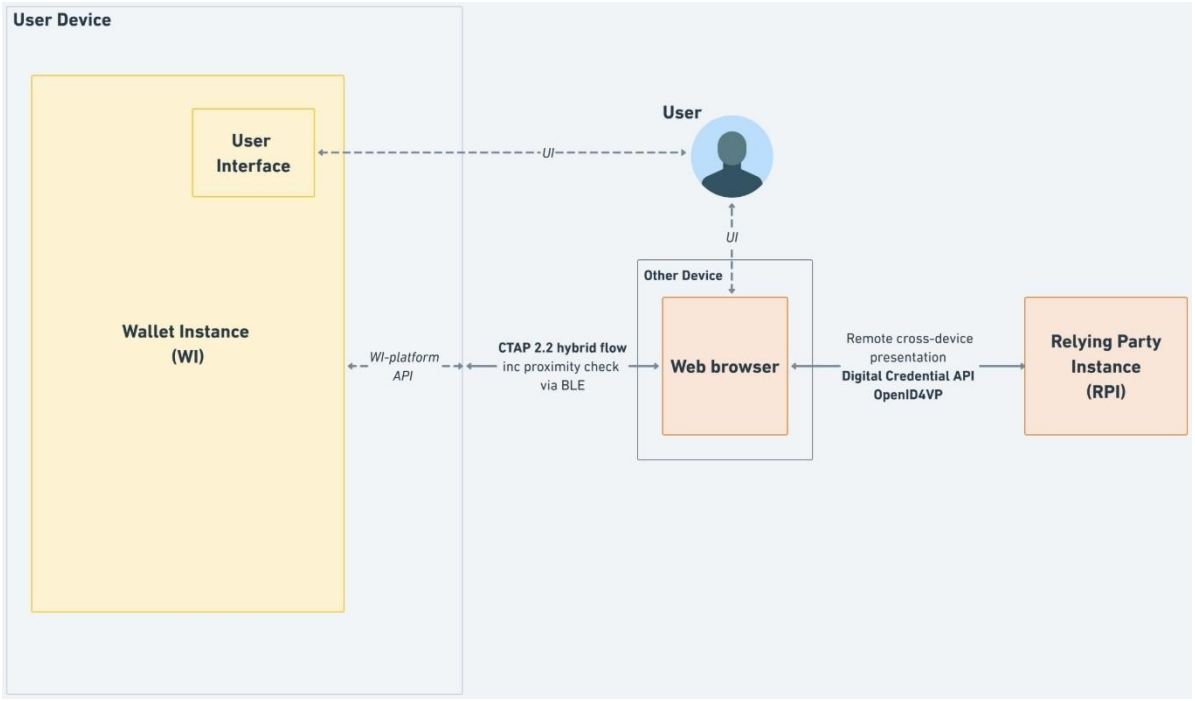

Figura 5: Presentaciones remotas entre dispositivos

Un flujo remoto de presentación de atributos entre dispositivos comienza cuando el Usuario utiliza un navegador en un dispositivo distinto de su dispositivo de Usuario para visitar el sitio web de la Parte usuaria (informada). El sitio web puede ofrecer al Usuario la posibilidad de presentar atributos de su Unidad Cartera, ejemplo haciendo clic en un botón. Si el Usuario hace, el navegador le pedirá permiso para conectarse a la Unidad Cartera. Si el Usuario lo permite, la Instancia de la Parte usuaria (informada) envía una solicitud de presentación al navegador a través de la API de Credenciales Digitales. El navegador establece entonces un túnel hacia el dispositivo del Usuario, utilizando el flujo híbrido FIDO CTAP 2.2, ver sección 11.5 de [CTAP]. Tenga en cuenta que este flujo también se utiliza para FIDO Passkeys. Esto se hace de la siguiente manera:

1. El navegador presenta un código QR que incluye información sobre el punto final del túnel, así como las claves que se utilizarán para establecer un canal seguro a través de este túnel.
2. El usuario escanea el código QR con la cámara de su dispositivo.
3. El dispositivo de usuario emite un anuncio BLE, que es recibido por el navegador. El anuncio incluye, de forma cifrada, la información necesaria para establecer el túnel seguro. Este anuncio se utiliza como comprobación de proximidad: el túnel no puede establecerse si el dispositivo de usuario y el dispositivo en el que se ejecuta el navegador no están cerca el uno del otro.
4. Se establece un túnel entre los dos dispositivos.

A continuación, el navegador envía la solicitud de presentación conforme con OpenID4VP al dispositivo de usuario. Si hay varias Instancias de Cartera presentes en el dispositivo del Usuario, el SO del dispositivo determinará a cuál de ellas se enviará la solicitud, posiblemente tras consultar al Usuario. La Instancia

Cartera seleccionada procesará la solicitud de presentación y, tras solicitar la aprobación del , devolverá los atributos solicitados en formato cifrado al , utilizando el túnel establecido. El navegador reenviará la respuesta a la Instancia Parte usuaria (informada) remota.

Nótese que la Instancia Cartera no ve ninguna diferencia entre el flujo entre dispositivos y el flujo en el mismo dispositivo. En ambos , recibe una solicitud de presentación compatible con OpenID4VP a través de la API de plataforma WI descrita en la sección anterior.

4.4.3.4 Perfilar el uso de [OpenID4VP] en los flujos de presentación remota

Como se ha mencionado anteriormente, tanto para los flujos de presentación remota en el mismo dispositivo como entre dispositivos, los mensajes utilizados para solicitar y presentar declaraciones cumplen con [OpenID4VP]. La OpenID Foundation está estandarizando un perfil para la API de credenciales digitales del W3C, que definirá cómo se utilizará OpenID4VP en esta API.

Además, hay otros dos perfiles que utilizarán las Unidades Cartera y las Partes usuarias (informadas) remotas:

- [ISO/IEC 18013-7] El Anexo B contiene un perfil para OpenID4VP. Las Partes usuarias y la Unidad Cartera cumplirán los requisitos de este perfil cuando el formato de la declaración se ajuste a [ISO/IEC 18013-5].
- En caso contrario, es decir, cuando el formato de la declaración se ajuste a [SD-JWT VC], las Partes usuarias y la Unidad Cartera cumplirán los requisitos del perfil especificado en [HAIP].

4.5 Tipos de arquitectura WSCD

4.5.1 Introducción

La figura 2 muestra cuatro tipos diferentes de arquitectura para el WSCD, que son:

- WSCD remoto
- WSCD local externo
- WSCD interno local
- Nativo local WSCD

Además, esta sección también describe una arquitectura híbrida. Dentro del ecosistema de Carteras IDUE, un Prestador de Carteras puede utilizar cualquiera de estas arquitecturas.

Tenga en cuenta que, independientemente de la arquitectura utilizada, el Prestador de Carteras es responsable de garantizar que la Instancia de Cartera pueda acceder a un WSCD que tenga un nivel de seguridad suficiente para garantizar que la Unidad de Cartera pueda alcanzar un Nivel de Aseguramiento "alto", tal y como exige el [Reglamento Europeo de Identidad Digital]. El Prestador de Carteras sigue siendo responsable de la gestión de las claves criptográficas en el WSCD (a través de la WSCA) durante toda la vida

útil de la Unidad de Cartera. El Prestador de Cartera también es responsable de certificar las propiedades del WSCD (incluidas las certificaciones pertinentes) en la Declaración de Unidad de Cartera, véase la sección 6.5.3.

4.5.2 WSCD remoto

En esta , el dispositivo criptográfico seguro de la Cartera está situado a distancia del dispositivo del Usuario. Normalmente, será implementado por el Proveedor de Carteras utilizando un HSM que se ejecuta en un servidor seguro. El Proveedor de Carteras también proporcionará la WSCA con la que interactúa la Unidad de Carteras.

Esta arquitectura se utiliza normalmente si el dispositivo del Usuario carece de hardware suficientemente seguro, o si el Proveedor de Carteras no quiere depender de dicho hardware.

4.5.3 WSCD local externo

Si el dispositivo de usuario carece de hardware suficientemente seguro, otra opción es utilizar un componente de hardware externo local como WSCD. Este WSCD externo local suele ser una tarjeta inteligente o un token seguro. Se conecta al dispositivo de usuario a través de NFC u otra conexión de corto alcance, y es capaz de realizar todas las operaciones criptográficas requeridas de un WSCD / WSCA en el ARF. Tenga en cuenta que muchas tarjetas inteligentes existentes, como los documentos de identidad, no podrán hacerlo.

La WSCA suele adoptar la forma de un applet de tarjeta Java. La WSCA se instala antes de expedir la tarjeta inteligente o el token seguro al usuario. El emisor de la WSCD y de la WSCA es el Prestador de Carteras u otra entidad que actúe en nombre del Prestador de Carteras o en cooperación con él.

4.5.4 WSCD interno local

En esta arquitectura, el dispositivo criptográfico seguro de Cartera se integra directamente en el dispositivo del usuario. Esto incluye soluciones como UICC, e-SIM/SAM o elementos seguros integrados.

Estas soluciones suelen ajustarse a las especificaciones de la tarjeta GlobalPlatform [GP CS] o a la especificación GSMA Secured Applications for Mobile [GSMA SAM].

La WSCA será normalmente un applet de tarjeta Java, y es emitida a distancia al WSCD por el Proveedor de Cartera, en el momento en que se activa la Unidad de Cartera; véase la Sección 6.5.3. Para ello, el Proveedor de Carteras puede necesitar conectarse y colaborar con otras entidades, como un Gestor de Servicios de Confianza empleado por el propietario del WSCD.

El Prestador de Cartera es responsable de verificar que el WSCD interno local todos los requisitos aplicables, antes de activar una Unidad de Cartera utilizando dicho WSCD.

4.5.5 Nativo local WSCD

En el dispositivo de usuario se integra un WSCD nativo local. Sin embargo, la API para acceder al WSCD está incluida en el sistema operativo del dispositivo de usuario. Por lo tanto, no necesaria una WSCA independiente. Alternativamente, la API ofrecida por el sistema operativo puede considerarse como la WSCA.

El Prestador de Cartera es responsable de verificar que el WSCD nativo local cumple todos los requisitos aplicables, antes de activar una Unidad de Cartera utilizando dicho WSCD.

4.5.6 Arquitectura híbrida

En esta arquitectura se combinan dos o más de los diferentes tipos de WSCD descritos anteriormente. Por ejemplo, un HSM remoto puede gestionar las claves criptográficas de la Unidad Cartera y de los DIP y declaraciones presentes en la Unidad Cartera, mientras que un Elemento Seguro integrado se utiliza para gestionar el acceso al HSM remoto.

4.6 Diagramas de estado

4.6.1 Introducción

En esta sección, se presentan diagramas de estado para Soluciones de Cartera, Unidades de Cartera, Proveedores de DIP y Proveedores de Declaraciones, DIP y declaraciones, y Partes usuarias.

4.6.2 Solución Cartera

Una Solución Cartera tiene su diagrama de estado. El estado de una Solución Cartera afecta al estado de todas las Unidades Cartera de esa Solución Cartera. La Figura 6 muestra los estados de la Solución Cartera:

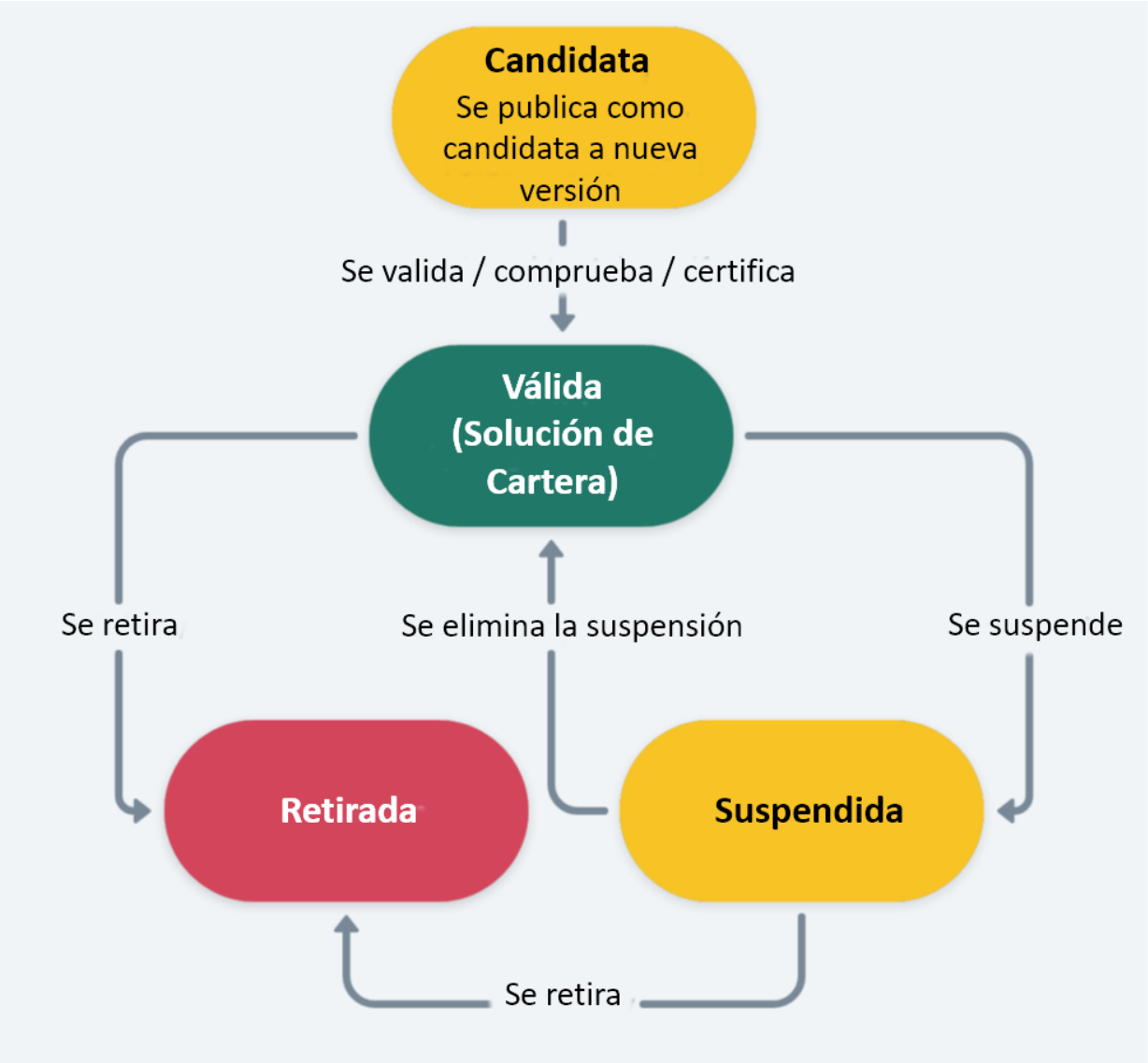

Figura **1:** Figura 6

Figura 6: Diagrama de estados de la solución Cartera

El estado **Candidato** es el primer estado de una Solución Cartera. Esto significa que está totalmente implementada

y el Prestador de Cartera solicita que la solución sea certificada como Solución de Cartera como parte de un esquema de eID de Cartera IDUE.

Si se han todos los criterios legales y técnicos, un Estado miembro puede decidir permitir que un Prestador de Carteras empiece a ofrecer la Solución Cartera a los Usuarios. El estado de la Solución Cartera pasa a ser **Válido**. Esto significa que la Solución Cartera puede ser lanzada oficialmente, y puede ser proporcionada a

los Usuarios. El Estado miembro emisor informa a la Comisión de cada cambio en el estado de certificación de sus sistemas de Cartera IDUE y de las Soluciones Cartera proporcionadas en el marco de ese sistema.

El Estado miembro emisor puede suspender temporalmente una Solución Cartera. Esto sería, por ejemplo, el resultado de un problema crítico de seguridad. Esto conduce al **Suspendido**. El Estado miembro emisor puede anular la suspensión de la solución Cartera, devolviendo la solución al estado **Válido**. El Estado miembro emisor también puede decidir retirar completamente la solución Cartera, lo que lleva a la solución Cartera al estado **Retirada**.

Una Unidad Cartera que forme parte de un Proveedor de Soluciones Cartera suspendido o retirado no podrá solicitar la emisión de un DIP o declaración. La Parte usuaria (informada) tampoco aceptará un DIP o declaración presentados por dicha Unidad Cartera.

4.6.3 Unidad Cartera

La figura 7 muestra los estados de una Unidad Cartera.

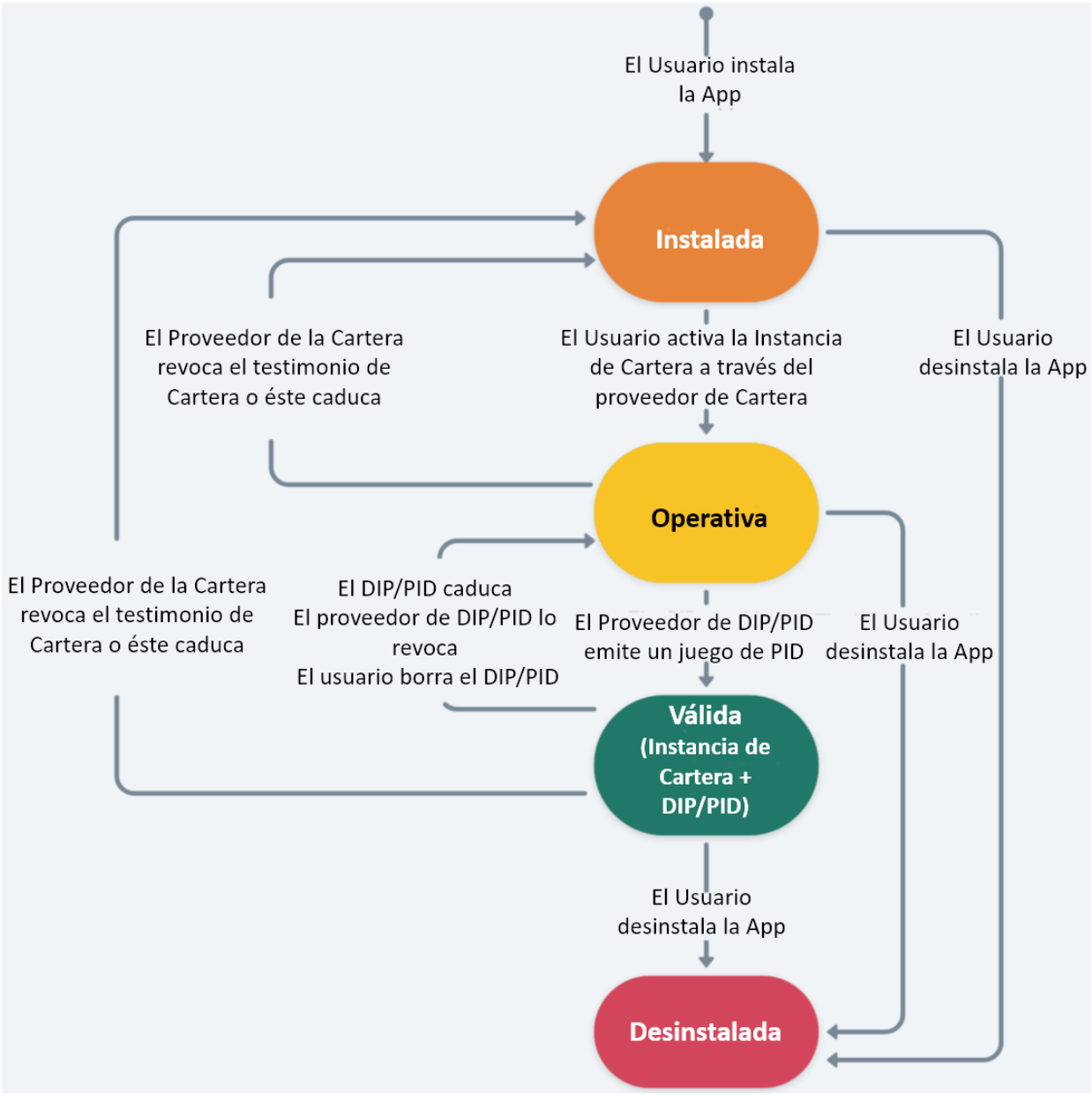

Figura **2:** Figura 7

Figura 7: Diagrama de estados de la unidad Cartera

El ciclo de vida de una Unidad Cartera comienza cuando el Usuario instala una Instancia Cartera en su dispositivo de Usuario, ver Sección 6.5.2. El estado de la Unidad Cartera es entonces **Instalada**. En este estado, el Usuario y el Prestador de Cartera sólo pueden realizar una acción, la activación de la Unidad Cartera, tal y como se describe en la Sección 6.5.3. Como parte del proceso de activación, el Prestador de Carteras emite uno o varios

Declaraciones de la Unidad Cartera (WUA) a la Unidad Cartera.

Una vez activada una Unidad Cartera, se encuentra en estado **Operativo**. En este estado, el Usuario y el Prestador de Cartera gestionan la Unidad de Cartera y pueden realizar las mismas acciones que en el estado **Válido**, véase más adelante. Sin embargo, obviamente, Usuario no puede identificarse ni autenticarse presentando un DIP a una Parte usuaria, ni puede ninguna otra acción con un DIP, porque por definición no hay ningún DIP válido en este estado.

Si, en el estado **Operativo**, un Proveedor de DIP emite un DIP a una Unidad Cartera, ésta pasa al estado **Válido**. Si, en cualquiera de estos dos estados, el Proveedor de Carteras revoca el PID o este expira, la Unidad Cartera vuelve a pasar a **Instalada**.

En el estado **Válido** se pueden realizar las siguientes acciones:

- El Prestador de Cartera actualiza la Unidad de Cartera a una nueva versión,
- El Prestador de Carteras revoca la Unidad Cartera, por ejemplo a petición del Usuario o si se rompe la seguridad de la Instancia Cartera. La revocación de la Unidad Cartera se realiza mediante la revocación de la Declaración de la Unidad Cartera (ver Tema 9 y Tema 38).
- El usuario solicita la emisión de un DIP, un DECA, un DEB-AAPP o un DEA-AAPP.
- El usuario presenta atributos de un DIP, una DECA, una DEB-AAPP o una DEA a una Parte usuaria (informada).
- El usuario elimina un DIP, una DECA, una DEB-AAPP o una DEA.
- Un DIP, un DECA, un DEB-AAPP o un DEA es revocado por su Prestador (si es válido durante más de 24 horas).
- El Usuario desinstala la Instancia Cartera.

Si el último o único DIP de la Unidad Cartera caduca, se revoca o se elimina, el estado de la Unidad Cartera vuelve a ser **Operativo**. Tenga en cuenta que si hay varios DIP en la unidad de cartera, ésta no pasa al estado **operativo** mientras al menos uno de ellos sea válido.

4.6.4 Prestador del DIP o proveedor de declaraciones

La figura 8 muestra los posibles estados de un Prestador de DIP o de un Proveedor de declaraciones.

Figura **3:** Figura 8

Figura 8: Diagrama de estado del Prestador de DIP o del Prestador de declaraciones

El estado **Válido** es el primer estado de un Proveedor de DIP o de un Proveedor de Certificados. Significa que ha sido registrado por el correspondiente Prestador de confianza y notificado a la , tal como se describe en la sección 6.3.2.

El Proveedor de listas de confianza puede suspender temporalmente a un Proveedor de DIP o a un Proveedor de declaraciones. Esto lleva al estado **Suspendido**. El Proveedor de la Lista de Confianza puede anular la suspensión del Proveedor de DIP o del Proveedor de Certificados, devolviéndolo al estado **Válido**. El Proveedor de la Lista de Confianza también puede decidir retirar completamente al Proveedor de DIP o al

Proveedor de Certificados, lo que lo lleva al estado **Retirado**. Para más información sobre la suspensión o retirada, consulte

Apartado 6.3.3. Un Proveedor de DIP o Proveedor de Certificaciones suspendido o retirado no podrá emitir DIP ni certificaciones para Unidades Cartera, ni las Partes usuarias aceptarán un DIP o una certificación emitidos por dicho Proveedor de DIP o Proveedor de Certificaciones.

4.6.5 DIP o declaración

La figura 9 muestra los posibles estados de un DIP o declaración.

En el contexto del ecosistema Cartera IDUE, un DIP o declaración comienza su ciclo de vida cuando se emite a una Unidad Cartera. Tenga en cuenta que esto significa que la gestión de atributos en la Fuente Auténtica (adhiriéndose a las estructuras nacionales y a las definiciones de atributos) está fuera del ámbito del ARF.

En determinados casos de uso, un DIP o una declaración pueden estar preaprovisionados, lo que significa que aún no son válidos cuando se expiden. En ese , su estado es **Emitido**, y pasará a **Válido** cuando llegue al comienzo de su período de validez. Sin embargo, si un DIP o una declaración se expide en fecha de inicio de validez o después, su estado cambia directamente a **Válido**.

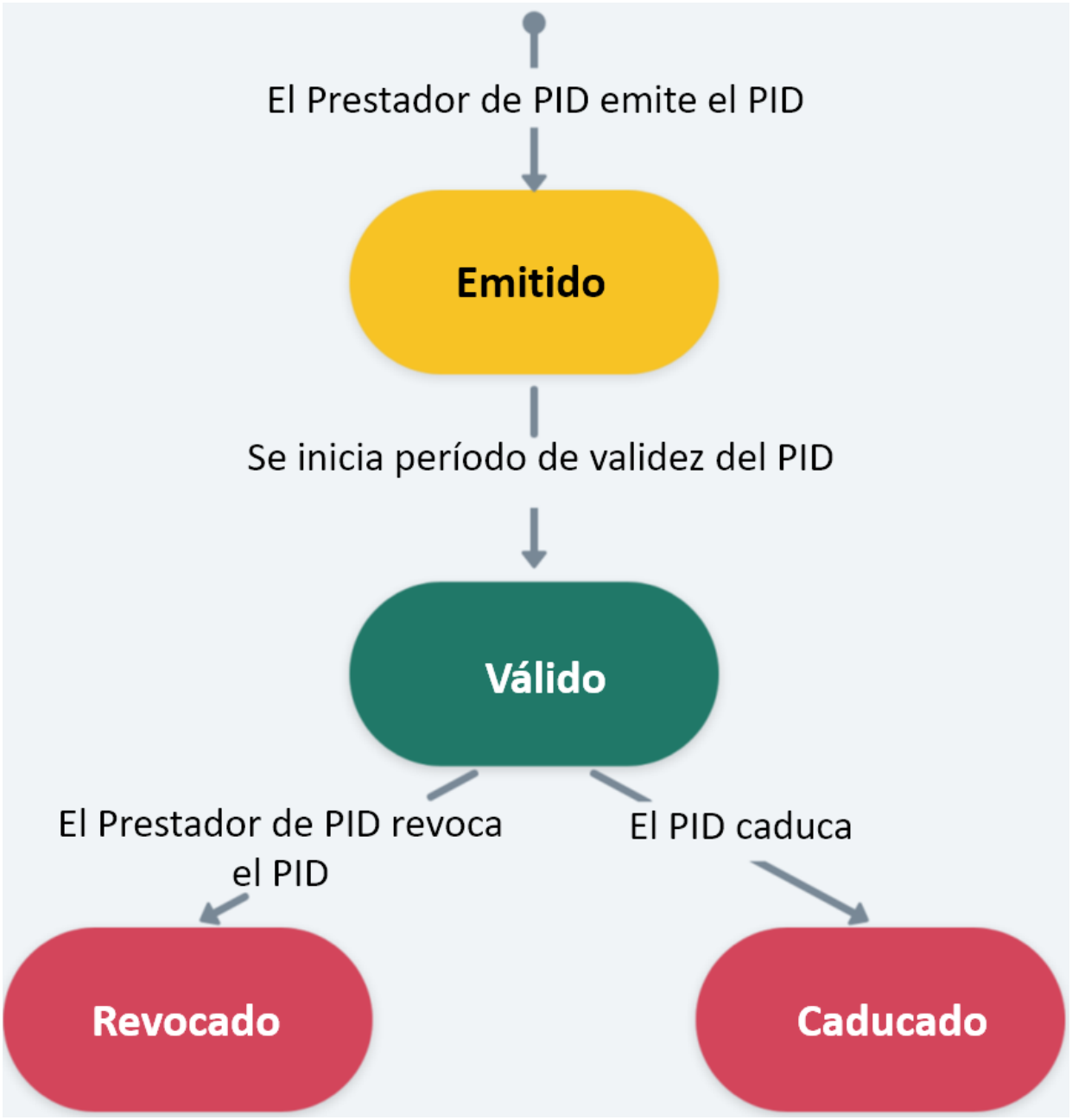

Figura **4:** Figura 9

Figura 9: Diagrama de estados del DIP o declaración

Existen dos transiciones posibles para un DIP o una declaración válidos: que caduquen al sobrepasar la fecha de fin de validez y pasen al estado **Caducado**, o que sean revocados por su Prestador de DIP o su Prestador de Declaración, terminando en el estado **Revocado**. La expiración y la revocación son transiciones independientes. Una vez que un DIP o una declaración han caducado o han sido revocados, no pueden volver al estado caducado o revocado.

a **Válido**.

4.6.6 Parte usuaria (informada)

La Figura 10 muestra los posibles estados de una Parte usuaria (informada).

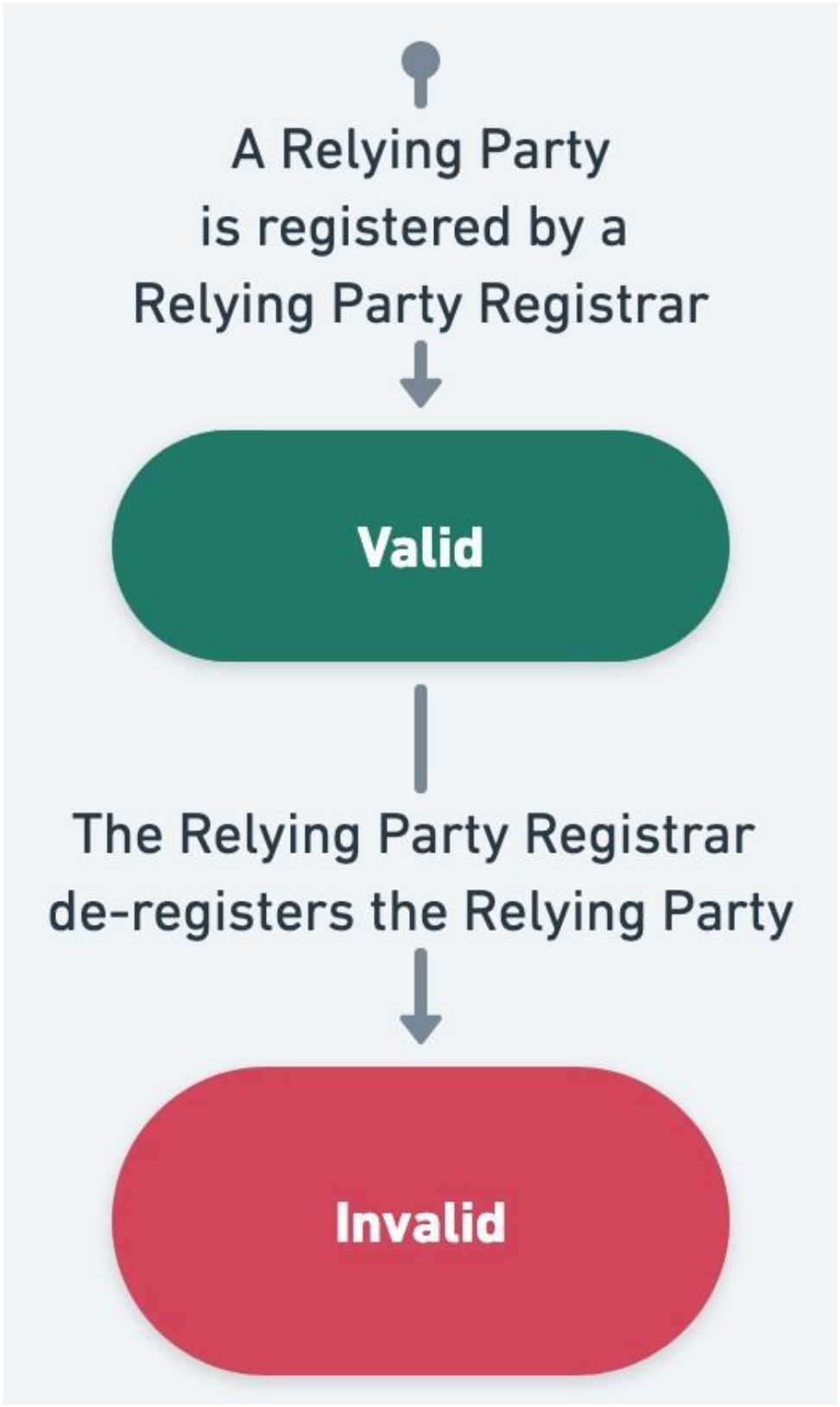
A Relying Party
is registered by a
Relying Party Registrar
Valid
The Relying Party Registrar
de-registers the Relying Party
Invalid

Figura **5:** Figura 10 Figura 9: Diagrama de estado de la Parte usuaria (informada)

El estado **Válido** es el primer estado de una Parte usuaria (informada). Significa que ha sido registrado por un Registrador de Parte usuaria, tal como se describe en el apartado 6.4.2.

El Registrador puede dar de baja a una Parte usuaria (informada). Esto conduce al estado **No válido**. Para obtener más información sobre la anulación del registro, consulte la sección 6.4.3. Una Unidad Cartera no presentará un DIP ni una declaración a una Parte usuaria (informada) que se encuentre en este .

4.7 Seudónimos

4.7.1 Introducción a las Passkeys

Como se especifica en [CIR 2024/2979], [W3C WebAuthn] define la especificación técnica de los seudónimos. Los pseudónimos son un tipo de credencial ampliamente utilizado que se crea y afirma utilizando la API WebAuthn.

Las claves de acceso deben considerarse una alternativa a las contraseñas. La idea es que un usuario, al registrar una cuenta de usuario en un servicio, utilice un dispositivo seguro para generar un par de claves pública y privada, registre la clave pública en el servicio y pueda utilizar posteriormente la clave privada para autenticarse en el servicio.

En un poco más de detalle, el flujo para utilizar Passkeys es el siguiente:

Inscripción:

1. El Usuario genera un par de claves pública-privada y almacena tanto la clave pública como la privada en su dispositivo seguro (denominado Autenticador).
2. El usuario registra la clave pública en el servicio de Parte usuaria (informada) deseado.

Autentificación:

1. Cuando el usuario desea autenticarse ante un servicio, éste le envía un desafío consistente en un valor aleatorio.
2. El usuario utiliza la clave privada almacenada en su Authenticator para firmar el reto y lo envía de vuelta al servicio.
3. El servicio comprueba que la firma del reto puede verificarse utilizando la clave pública registrada. Si la firma se verifica y el origen coincide con esperado, se considera que el usuario está autenticado y se le concede acceso al servicio.

4.7.2 Introducción a [W3C WebAuthn]

4.7.2.1 Visión general

[W3C WebAuthn] define una API para la creación y uso de Passkeys. Conceptualmente, además del Usuario, hay cuatro componentes lógicos diferentes en esta especificación:

- **Servidor de la Parte usuaria (informada):** La Parte usuaria (informada) que desea ofrecer un servicio basado en la auten- ticación mediante Passkeys.
- **Parte usuaria (informada):** El programa proporcionado por la Parte usuaria que se ejecuta en el Cliente del usuario y se comunica con el Servidor de la Parte usuaria. El Cliente de la Parte usuaria es normalmente un código JavaScript, proporcionado por la Parte usuaria, que se ejecuta en el Cliente (es decir, en el navegador).
- **Cliente:** El cliente que el usuario utiliza para interactuar con el servidor de la Parte usuaria y con el autenticador del . El Cliente puede considerarse como el navegador que el Usuario utiliza para acceder al servicio de la Parte usuaria.
- **Autenticador:** El dispositivo controlado por el Usuario para crear, almacenar y utilizar las Claves de Acceso. En el contexto de la Cartera IDUE, la Unidad de Cartera es el Autenticador.

Tenga en cuenta que el Cliente de Parte usuaria y el Cliente son dos programas que se ejecutan en la misma máquina física.

[W3C WebAuthn] define un modelo que divide las responsabilidades entre estas diferentes entidades y define una interfaz entre la Parte usuaria (informada) y el Cliente. Además, define un protocolo de desafío/respuesta para autenticar con Passkeys. La interfaz se denomina *WebAuthn API*.

Sin embargo, [W3C WebAuthn] no especifica cómo deben comunicarse el Autenticador y el Cliente.

[W3C WebAuthn] se basa en varios tipos diferentes de identificadores, entre ellos:

- **ID de la Parte usuaria (informada):** Un identificador único de la Parte usuaria, que debe ser una cadena de dominio válida. El usuario identificará así a la Parte usuaria y el Autenticador sabrá qué Parte usuaria solicita el registro o la autenticación.
- **ID de credencial**: Identificador único elegido por el Autenticador para cada Passkey.
- **ID de Usuario:** Un identificador único para cada Usuario, que es asignado por la Parte usuaria (informada). Se proporcionará al autenticador al registrar una nueva clave de acceso. Posteriormente, será facilitado por el Autenticador al autenticarse ante la Parte usuaria. El autenticador llevará un registro de qué claves están disponibles para qué ID de usuario e ID de Parte usuaria (informada). La Parte usuaria guarda un nombre de usuario para cada ID de usuario.
- **Nombre de usuario:** Un alias que puede ser elegido por el Usuario o la Parte usuaria y asignado a una Clave de acceso específica en el Autenticador. Esto permite al usuario distinguir y seleccionar fácilmente la clave con la que desea autenticarse, si hay varias en el autenticador para la Parte usuaria en cuestión.

En las siguientes secciones se explica cómo funcionan conjuntamente los distintos componentes para permitir el registro y la posterior autenticación mediante Passkeys.

4.7.2.2 Inscripción

El flujo para registrar una Passkey en [W3C WebAuthn] es el siguiente:

0. El Usuario solicita (fuera de banda de WebAuthn) a la Parte usuaria (informada) que cree un nuevo Seudónimo.
1. El servidor de la Parte usuaria crea una impugnación y la envía junto con el ID de usuario, el ID de la Parte usuaria y el nombre de usuario al cliente de la Parte usuaria.
2. La Parte usuaria (informada) reenvía la información al Cliente mediante la WebAuthnAPI.
3. El Cliente comprueba que el ID de la Parte usuaria (informada) coincide con el origen de la llamada y envía la información al Autenticador junto con otros datos contextuales.
4. El Autenticador autentica al Usuario (por ejemplo utilizando un PIN o mediante biometría). A continuación, genera un nuevo par de claves con un nuevo ID de credencial y establece el alcance del mismo en el ID de Parte usuaria y el ID de usuario específicos. Por último, el Autenticador puede generar una declaración (explicada en la Sección 4.7.2.3) y enviarla, junto con la clave pública y su ID de credencial, al Cliente.
5. A continuación, el Cliente reenvía la información al Cliente Parte usuaria que, a su vez, la reenvía al Servidor Parte usuaria.
6. El servidor de la Parte usuaria verifica la declaración (si existe) y registra la clave pública recibida para este ID de usuario.

Obsérvese que el Autenticador almacena la clave pública de forma que se asigna únicamente a Parte usuaria específica, de acuerdo con los requisitos del artículo 14 (2) del [CIR 2024/2979], que establece que los seudónimos deben ser únicos para cada Parte usuaria (informada).

4.7.2.3 Declaración de seudónimo

El término "declaración" se utiliza aquí de forma diferente que en otras partes del ARF. En este contexto, la declaración no se refiere a los atributos del usuario, sino a los atributos del autenticador.

La declaración sirve para garantizar a la Parte usuaria que está hablando con un Autenticador con ciertos atributos. La declaración suele adoptar la forma de una firma en el reto, así como otros datos contextuales.

En [W3C WebAuthn] se mencionan cinco tipos diferentes de declaraciones:

- **Declaración básica:** El autenticador almacena una única maestra pública y privada. La clave privada se utiliza para firmar todas las declaraciones y se incluye un certificado sobre la clave pública en los datos de la declaración para que la Parte usuaria (informada) pueda verificar la firma.

- **Declaración CA:** Similar a la anterior, en el sentido de que el autenticador una única clave maestra pública y privada. Sin embargo, en lugar de utilizarla para atestiguar claves de paso, el autenticador la utiliza para autenticarse ante una autoridad de certificación (CA), que a su vez está configurada para emitir certificados al autenticador sobre múltiples pares de claves de declaración.

- **CA de anonimización:** Similar al segundo punto anterior, salvo que se explicita que el Autenticador solicita un certificado para un nuevo par de claves de declaración por cada Passkey generada.

- **Autodeclaración:** La declaración se firma con la clave privada del par de claves recién generado en la Passkey. Tenga en cuenta que esto no ofrece ninguna garantía a la Parte usuaria (informada) sobre el Autenticador con el que está interactuando.

- **No se da declaración de atestado:** No se proporciona ninguna declaración. Tenga en cuenta que esto no ofrece ninguna garantía a la Parte usuaria (informada) sobre el Autenticador con el que está interactuando.

Tenga en cuenta que el artículo 5a (5) a) viii) del [Reglamento Europeo de Identidad Digital] establece que *"las Carteras de Identidad Digital Europeas soportarán, en particular, protocolos e interfaces comunes: ... para que las partes usuarias verifiquen la autenticidad y validez de las Carteras de Identidad Digital Europeas;...* ". Las dos últimas formas de declaración no se ajustan a este requisito. La sección 5.1 del documento de debate para el Tema E analiza cómo las otras tres posibilidades se relacionan con los riesgos para la privacidad sobre la vigilancia del usuario identificados en la sección 7.4.3.5.

4.7.2.4 Autenticación

El flujo para la autenticación utilizando una Passkey siguiendo [W3C WebAuthn] es:

1. El servidor de la Parte usuaria crea una impugnación y la envía junto con su ID de Parte usuaria al cliente de la Parte usuaria.
2. La Parte usuaria (informada) reenvía la información al Cliente mediante la API WebAuthn.
3. El Cliente comprueba que el ID de la Parte usuaria (informada) coincide con el origen de la persona que llama y envía la información al Autenticador junto con otros datos contextuales. 4. El autenticador autentica al usuario (por ejemplo, mediante un PIN o datos biométricos). A continuación, pide al usuario que seleccione una de las claves de acceso asignadas a esta Parte usuaria ID (informada), si hay varias. Para este paso se puede presentar al Usuario el Nombre de Usuario. Por último, el autenticador utiliza la clave privada del par de claves elegido (= clave de acceso) para firmar la impugnación, así como algunos datos contextuales, como el ID de usuario, el ID de credencial y el ID de la Parte usuaria (informada). A continuación, el autenticador lo envía al cliente.
5. El Cliente reenvía la información al Cliente Parte usuaria, que a su vez la reenvía al Servidor Parte usuaria.

6. El servidor de la Parte usuaria (informada) verifica la firma con la clave pública almacenada para este ID de usuario e ID de credencial y, en función del resultado de esta verificación, considera que el usuario está autenticado.

5 Modelo de datos

5.1 Introducción

En el ecosistema de la Cartera IDUE, los datos se intercambian en forma de Declaraciones Electrónicas de Atributos (DEA), en lo sucesivo denominadas "declaraciones." Además de los DEA, el [Reglamento Europeo de Identidad Digital] define explícitamente otra categoría de datos, denominada Datos de identificación Personal (DIP), que establece la identidad de una persona física o jurídica. El DIP sólo puede ser expedido por un Prestador de DIP que opere bajo la supervisión del Estado miembro. Cada DIP y declaración consta de los siguientes elementos clave:

- Conjunto de **atributos** que proporcionan información sobre el sujeto de la declaración. El sujeto del DIP o de la declaración puede ser una persona física o . Una Parte usuaria (informada) solicitará uno o varios de estos atributos para obtener la información fiable que necesita para prestar algún servicio al . El conjunto de atributos que puede contener una declaración se define en un esquema de atributos, véase más abajo.

- Conjunto de **metadatos**, es decir, información sobre la propia declaración, como su tipo de declaración (DIP, Carné de Conducir Móvil (CCm), título, etc.), su Prestador de servicios de certificación y su período de validez administrativa, si procede. Este tipo de metadatos también se define en un esquema de atributos. Además, los metadatos también incluyen la información necesaria para garantizar la seguridad

  de la declaración. Esto incluye al menos su período de validez técnica. También incluye una clave pública del certificado, que la Parte usuaria (informada) utilizará para verificar que el certificado no ha sido copiado (véase la sección 6.6.3.8). También puede incluir información que permita a la Parte usuaria (informada) verificar que la declaración no ha sido revocada (véase la sección 6.6.3.7).

- Una **prueba** que garantice la integridad, la autenticidad y el apoyo a la divulgación selectiva de la declaración. El formato de la prueba se ajusta al mecanismo de prueba especificado para este tipo de declaración (véase más adelante). La prueba incluye información que permite a una Parte usuaria (informada) verificar la prueba, por ejemplo, un certificado de Prestador de servicios de certificación y una referencia a un anclaje de confianza que puede utilizarse para verificar dicho certificado.

Un **esquema de atributos** define la organización lógica de todos los atributos obligatorios y opcionales de una declaración, así como el formato de cada atributo, es decir, su identificador único, codificación, valores permitidos y serialización. Además, un esquema de atributos especifica algunos de los metadatos de la declaración, como el tipo de declaración e información sobre su Prestador de Declaraciones, período de validez, etc. En el ecosistema de la Cartera IDUE, el esquema de atributos para cada tipo de declaración es

especificado por un Prestador de Esquema de Atributos en una Directrices de elaboración de declaraciones, de acuerdo con la Sección 5.5.

Un **mecanismo de prueba** define el método utilizado para crear la prueba de declaración. Por ejemplo, una firma digital "estándar" es una prueba que garantiza la integridad y la autenticidad, pero no permite la divulgación selectiva. Los mecanismos de prueba se especifican en normas o especificaciones técnicas. Los formatos de declaración enumerados en la sección 5.4 especifican un mecanismo de prueba que permite la divulgación selectiva o dejan que hagan otras especificaciones técnicas.

5.2 Categorías de declaración

Dentro del ecosistema de la Cartera de Identidad Digital Europea, la [Regulación de la Identidad Digital Europea] distingue cuatro categorías legales de declaraciones, que se definen del siguiente modo:

- **Datos de identificación Personal (DIP**): Conjunto de datos que se expide de conformidad con el Derecho de la Unión o nacional y que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a otra persona física o .
- **Declaración Electrónica Cualificada de Atributos (DECA**): Declaración Electrónica de Atributos emitida por un Prestador de Servicios de Confianza Cualificado (QTSP) y que cumple los requisitos establecidos en el Anexo V del Reglamento.
- **Declaración Electrónica de Atributos expedida por o en nombre de un organismo del sector público responsable de una fuente auténtica (DEA-A**APP): Declaración Electrónica de Atributos expedida por un organismo del sector público responsable de una fuente auténtica o por un organismo del sector público designado por el Estado miembro para expedir dichas declaraciones atributos en nombre de los organismos del sector público responsables de las fuentes auténticas de conformidad con el artículo 45 septies y con el anexo VII del Reglamento.
- **DEA no calificada:** Una CEA que no es CEA ni DEA-AAPP.

Tenga en cuenta que las diferencias entre estas categorías de declaración son puramente jurídicas. Por ejemplo, un diploma puede ser un DECA o un DEA no cualificado, dependiendo de si es emitido por un proveedor de servicios de confianza cualificado (QTSP) o por uno no cualificado. Del mismo modo, un carné de conducir móvil puede ser un DEA-AAPP, un DEA-Q o un DEA-no cualificado, dependiendo del estatuto jurídico de la parte que expide los carnés de conducir móviles en cada Estado miembro. Desde un punto vista técnico, todos los DIP, QEAA, PuB-EAA y DEA cumplen uno de los formatos de declaración enumerados en la sección 5.4.

5.3 Datos de identificación Personal

Además de que el Reglamento define el DIP como una categoría de datos jurídicamente distinta de las DEA, otra diferencia entre el DIP y las DEA es que la presencia o ausencia de un DIP válido determina si una Unidad Cartera se encuentra en estado Operativo o Válido, como se expone en el apartado 4.6.3.

Como se indica en esa sección, es posible que una Unidad Cartera contenga varios DIP. Si el usuario tiene varias nacionalidades, puede recibir un DIP de varios Prestadores de DIP en una única Unidad Cartera. Sin embargo, tenga en cuenta que un Proveedor de Carteras es libre de decidir que su Unidad Cartera no admite todos los Proveedores de DIP y que, a la inversa, un Proveedor de DIP puede decidir que no admite todas las Soluciones Cartera; véase la Sección 6.5.2.3. Obsérvese que el sujeto de todos los DIP de la Unidad Cartera será la misma persona, a saber, el Usuario de la Unidad Cartera.

5.4 Formatos normalizados de declaración

En el ecosistema de la Cartera IDUE se utilizan (potencialmente) los siguientes formatos normalizados adecuados para las declaraciones electrónicas de atributos:

1. La norma ISO/IEC 18013-5 define un esquema de atributos, un formato de datos y mecanismos de prueba para los permisos de conducción móviles, que pueden utilizarse también para otros tipos de declaraciones, véase [ISO/IEC 18013-5].
2. SD-JWT-based Verifiable Credentials (SD-JWT VC) define un mecanismo de prueba similar a [ISO/IEC 18013-5], pero para un formato de datos diferente, véase [SD-JWT VC].
3. W3C Verifiable Credentials Data Model v1.1 [W3C VC DM v1.1] define un esquema de atributos genérico independiente de formatos de datos y mecanismos de prueba, mientras que v2.0 introduce requisitos sobre formato y recomendaciones sobre mecanismos de prueba, véase [W3C VC DM v2.0].

Véanse los capítulos 3 y 4 del Documento de Debate del Tema V para más consideraciones sobre estos formatos y su interoperabilidad dentro del ecosistema Cartera IDUE.

El tema 12 establece los requisitos relativos a la compatibilidad con estas especificaciones.

5.5 Directrices de elaboración de declaraciones

Esta sección especifica el concepto de Directrices de elaboración de declaraciones. Para cada tipo de declaración, como un DIP, un Carné de Conducir Móvil (CCm), un diploma o una receta electrónica, un Manual de normas de certificación especifica el esquema de atributos y los mecanismos de prueba de esa declaración y, cuando sea necesario, los mecanismos de confianza para la autenticación y la autorización. Cada declaración tiene un tipo de declaración. El esquema de atributos especificado en el Manual de normas de certificación define el identificador único, la sintaxis y la semántica de todos los atributos que pueden formar parte de esa declaración.

Las Directrices de elaboración de declaraciones también establecen algunas opciones relativas a los protocolos de presentación que deben respaldar las declaraciones correspondientes. El Tema 12 contiene los requisitos para las Directrices de elaboración de declaraciones.

Las Directrices de declaración son definidas por los Prestadores de Esquema de Atributos, véase el apartado 3.15. Esta función puede ser asumida por distintos tipos de organizaciones:

- Algunas Directrices de elaboración ya han sido definidas por la Comisión Europea, en consulta con el Grupo Europeo de Cooperación en materia de Identidad Digital (EDICG). Se trata de las Directrices elaboración del DIP dedel Carné de Conducir Móvil (CCmy) del Anexo 3 del ARF. • Las Directrices de elaboración de una declaración destinada a ser utilizada en varias organizaciones o a través de las fronteras pueden ser definidas por una organización en la que, en la medida de lo posible, estén representadas todas las partes interesadas. Esto evitará que se definan varias Directrices de elaboración para el mismo tipo de declaración, por ejemplo, diplomas. También evitará diferencias innecesarias en la sintaxis y la semántica entre declaraciones similares. La decisión sobre

  qué organización será responsable de una determinada Directrices de elaboración de declaraciones queda fuera del ámbito de este documento. Como se explica en el Tema 12, es posible que un Prestador de Certificados individual necesite incluir atributos en una declaración que no se hayan especificado en las Directrices de elaboración sectoriales o comunitarias pertinentes. Un ejemplo de ello son los atributos que sólo tienen significado en el Estado miembro en el que reside el Prestador de Certificados. Para permitir este tipo de atributos nacionales, un Prestador de servicios de certificación puede definir unas Directrices de elaboración personalizadas para especificar atributos que son específicos de este Prestador y que no están incluidos en las Directrices sectoriales o de la UE.
- Las Directrices de elaboración de una declaración destinada a ser utilizada únicamente dentro de una organización serán definidas por dicha organización.

5.6 Catálogos

La sección 2 del artículo 45 sexies del Reglamento establece la base jurídica directa para que la Comisión "en caso necesario, establezca especificaciones y procedimientos para el catálogo de atributos y sistemas de declaración de atributos y procedimientos de verificación para las Declaraciones Electrónicas Cualificadas de Atributos".

Una de las principales razones del ARF es alcanzar un alto nivel de interoperabilidad. Esta interoperabilidad puede lograrse a diferentes niveles. A nivel técnico, la interoperabilidad puede lograrse utilizando normas, protocolos y especificaciones técnicas comunes, garantizando un lenguaje común para los Prestadores de servicios de certificación, los Prestadores de servicios de cartera y las Partes usuarias, permitiendo la emisión, presentación y procesamiento de declaraciones, sobre la base de protocolos, interfaces y sintaxis comunes acordados.

La otra capa es la semántica y se refiere a los esquemas semánticos de los atributos. El riesgo es que una forma incontrolada de implementación y uso creará barreras y complicará la implementación, con lo que el

ecosistema será mucho más costoso de crear y mantener, complejo y sensible a los errores, lo que afectará a la calidad del sistema global.

Para el desarrollo y el éxito del ecosistema Cartera IDUE, la reutilización de los componentes básicos de atributos y declaraciones es, por tanto, esencial. La creación y el mantenimiento de vocabularios controlados, un catálogo de atributos y unas Directrices de elaboración de declaraciones permiten acortar los plazos de comercialización y lograr una aplicación eficaz.

Partiendo de los requisitos del Tema 12 y teniendo en cuenta, por un lado, la necesidad de interoperabilidad y, por otrola variada naturaleza de las declaraciones y organizaciones que especifican dichas declaraciones, se definieron los siguientes principios:

- Las Directrices de elaboración de declaraciones para las DEA y DEA-AAPP utilizadas en el ecosistema de la Cartera IDUE podrán registrarse y publicarse en un catálogo de acceso público. El catálogo de normas de declaración también podrá incluir normas de declaración para DEA no cualificadas.
- La Comisión tomará medidas para establecer y mantener el catálogo de Directrices de declaración.
- El catálogo de Directrices de elaboración de declaraciones permitirá a los Prestadores de declaraciones, Partes usuarias y otros agentes del ecosistema de Carteras IDUE saber qué tipos de declaraciones existen y cuáles son los identificadores, la sintaxis y la semántica de todos los atributos que forman parte de la declaración.

También se hace hincapié en los siguientes puntos, para facilitar la creación y adopción:

- El registro de una Directrices de elaboración en el catálogo de Directrices de elaboración no es obligatorio.
- El registro no crea ninguna obligación ni aceptación automática por parte de terceros, ni implica automáticamente el reconocimiento transfronterizo del tipo de declaración descrito en las Directrices de elaboración.
- El catálogo de Directrices de elaboración puede estar en el mismo entorno que el catálogo de atributos.

La aplicación de estos principios se debatirá con más detalle. La ambición es utilizar los esfuerzos y herramientas existentes creados por los Estados miembros, la Comisión y las organizaciones transfronterizas, para conectar e interactuar con las partes interesadas, utilizar los activos de datos existentes para actualizarlos cuando sea necesario y añadir nuevos conjuntos de datos para apoyar nuevos casos de uso que se implementarán en el ecosistema de Cartera IDUE.

Los Temas 26 25 y presentan la situación actual y prevista de los catálogos, su creación, distribución, localización, gestión y mantenimiento, que permitirán procedimientos de actualización sencillos, sin sobrecargar el proceso, por una parte, garantizando al mismo tiempo mecanismos coherentes y permanentes para mantener los catálogos actualizados y accesibles para los agentes pertinentes, tanto los que crean el contenido como los que utilizan, consumen y procesan los atributos y las declaraciones, y por último, pero no por ello menos importante, para el público en general.

6 Modelo de confianza

6.1 Alcance

El modelo de confianza presentado en este capítulo define cómo se establece, mantiene, valida y gestiona la confianza entre las entidades del ecosistema de Cartera IDUE. Esboza las reglas, suposiciones y mecanismos subyacentes que rigen las relaciones de confianza, determinando si una entidad (como una Unidad Cartera, Dispositivo usuario o Parte usuaria (informada)) puede considerarse digna de confianza.

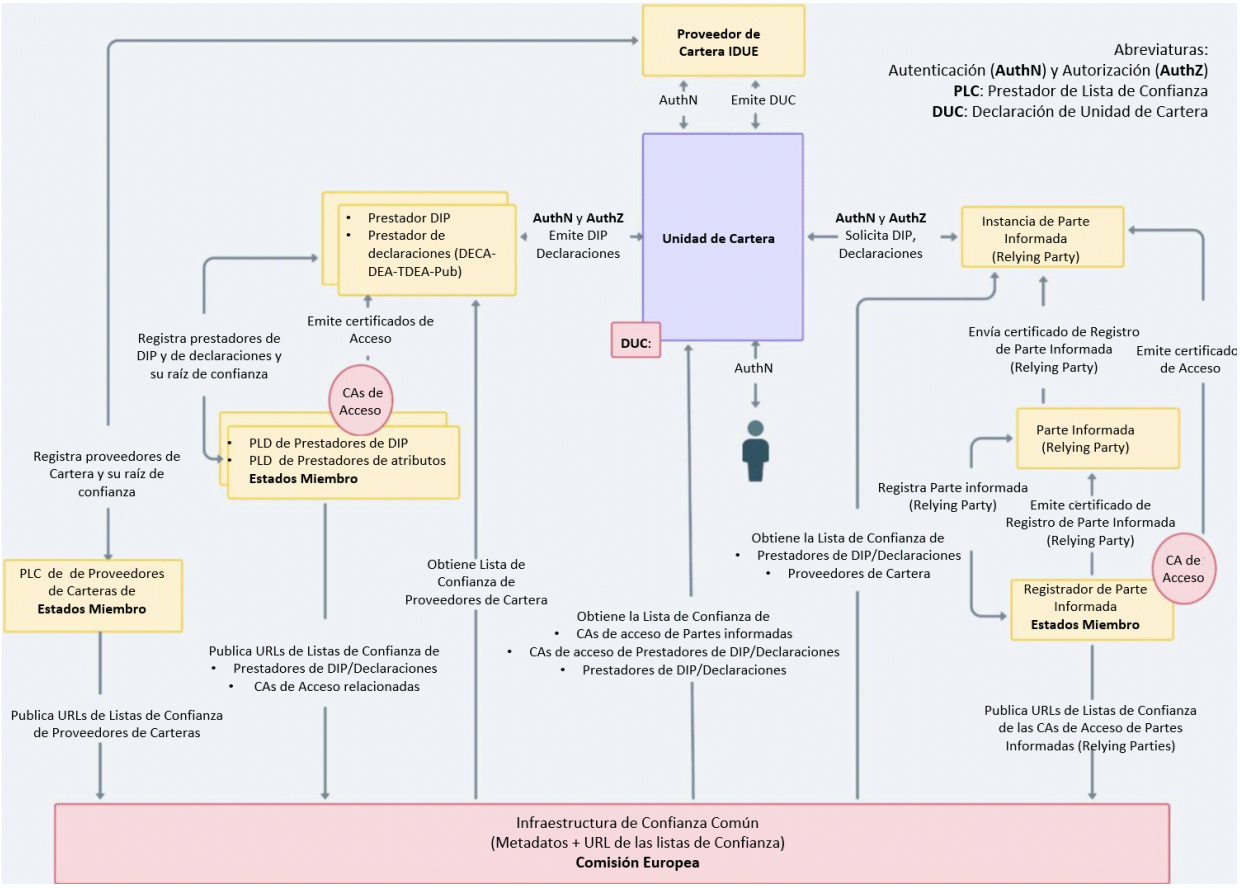

Figura **6:** Figura 11

La figura 11 ilustra las entidades clave y las relaciones en el modelo de confianza del ecosistema Cartera IDUE.

Su núcleo es la **Unidad Cartera** (arriba en el centro, azul), que interactúa con varias entidades a lo largo de su ciclo de vida. El ciclo de vida de la Unidad Cartera se detalla en la Sección 6.5 y consiste en la instalación, activación, gestión y desinstalación. Cada Unidad de Cartera es una configuración de una **Solución de Cartera**, que comprende una **Instancia de Cartera** y uno o más WSCA/WSCD, proporcionada por un **Prestador de Carteras**. El Proveedor de Carteras supervisa estos componentes y gestiona su registro, retirada o suspensión (véase la Sección 6.2). El Proveedor de Cartera garantiza que una Unidad de Cartera

válida posee al menos una **Declaración de Unidad de Cartera (WUA**), para permitir a otras entidades autenticar la Unidad de Cartera. El Prestador de Carteras puede revocar los WUA en caso necesario.

La unidad Cartera gestiona **los DIP de usuario** y **las declaraciones** (QEAA, DEA-AAPP y DEA-AAPP no cualificadas). **Los D**IP son emitidos **por Proveedores de DIP** y las declaraciones por **Proveedores de Declaraciones**, ambos situados a la izquierda de la Unidad Cartera en la Figura 11. Antes de interactuar con una Unidad Cartera, estos proveedores deben estar registrados en un **Proveedor de DIP Proveedor de Listas de Confianza (TLP)** o **Proveedor de atestaciones TLP**. Una vez registrados, reciben un **certificado de acceso** de una **CA de acceso de proveedor de DIP** o **de una CA de acceso de proveedor de atestación**. Véase el apartado 6.3.

Una vez que una Unidad Cartera recibe un DIP o una declaración, puede presentar atributos **de usuario** a las **Instancias de la Parte usuaria** (**informada**) (parte derecha de la Figura 11). Estas instancias son configuraciones de hardware/software que permiten a **las Partes usuarias** interactuar con las Unidades Cartera. Las Partes usuarias se registran en un **Registrador de Partes usuarias**, recibiendo un **certificado de acceso** para cada Instancia de Parte usuaria, así como **un Certificado de registro de Parte usuaria**. Esto se trata en la Sección 6.4.

En la sección 6.6 se detalla el ciclo de vida de los DIP y las declaraciones, incluida su emisión, presentación, gestión y eliminación.

Notas:

- Este modelo conceptual de confianza puede aplicarse con ligeras variaciones en los distintos Estados miembros, como la adopción de una o varias Autoridades de Certificación o el aprovechamiento de entidades existentes que ya cumplen esta función.
- Para los certificados de acceso, los DIP, las DEA cualificadas y las DEA-AAPP, la interoperabilidad es esencial (sección 4.2.2) y se consigue utilizando una PKI que siga las normas de certificados X.509 (RFC5280, RFC3647). Las DEA no cualificadas pueden adoptar modelos de confianza y mecanismos de verificación alternativos.
- El modelo admite casos de uso tanto remotos como de proximidad, aunque las medidas técnicas y los mecanismos de autenticación pueden variar.
- Esta versión del ARF aún no incluye interacciones de confianza para **firmas electrónicas cualificadas o sellos** (véanse los 16 Temas 37 y del Anexo 2).
- Además de las relaciones de confianza descritas en este , también se establecen otras relaciones de confianza. Por ejemplo, los usuarios, los Prestadores de DIP, los Prestadores de declaración y los Prestadores de confianza.

  Las partes confían en los organismos de certificación y en los Prestadores de Listas de Confianza. Esta confianza se basa principalmente en la autoridad y en medidas de procedimiento, como la supervisión pública, las políticas operativas y de seguridad publicadas y las auditorías, más que en medidas técnicas. Para verificar que las entidades interactúan realmente con una autoridad de confianza, se utilizarán medidas técnicas estándar adecuadas al contexto.

6.2 Confianza a lo largo del ciclo de vida de una solución Cartera

6.2.1 Ciclo de vida de la solución Cartera

La sección 4.6.2 presenta el ciclo de vida de una solución Cartera:

1. El Proveedor de Carteras responsable de la Solución Cartera es registrado por un Proveedor de Listas de Confianza. Como resultado, la Solución Cartera entra en estado Válido. Esto se trata en la sección 6.2.2.
2. Bajo condiciones específicas, un Proveedor de Listas de Confianza puede decidir suspender o retirar a un Proveedor de Carteras registrado. Esto se trata en la sección 6.2.3.

6.2.2 Registro y notificación del Prestador de Cartera

La figura 11 muestra al Prestador de Cartera en la parte superior de la Unidad de Cartera. A la izquierda y debajo de ésta, la figura también muestra que un Proveedor de Cartera se registra a sí mismo y a su Solución de Cartera con un Proveedor de Cartera de la Lista de Confianza en su Estado Miembro. Posteriormente, el Estado miembro notifica el Proveedor de Cartera a la Comisión Europea.

La Solución Cartera proporcionada por el Prestador de Carteras está certificada tal y como se describe en el Capítulo 7.

Si los procesos de registro y notificación tienen éxito, las anclas de confianza del Proveedor de Carteras se incluyen en una Lista de Confianza de Proveedores de Carteras. Durante la emisión de un DIP o una declaración, el Proveedor de DIP o el Proveedor de Declaraciones pueden utilizar estas anclas de confianza para verificar la autenticidad de una Declaración de Unidad Cartera firmada por el Proveedor de Carteras, de modo que puedan estar seguros de que están tratando con una Unidad Cartera auténtica de un Proveedor de Carteras de confianza. Ver Sección 6.6.2.3, Tema 9 y Tema 38. Del mismo modo, cuando la Unidad Cartera presenta un DIP o una declaración a una Parte usuaria, ésta puede utilizar las anclas de confianza del Proveedor de Cartera para verificar la autenticidad de una Declaración de Unidad Cartera firmada por el Proveedor de Cartera; véase la Sección 6.6.3.11, Tema 9 y Tema 38.

Si una determinada entidad ofrece múltiples Soluciones Cartera, se registrará como Prestador Cartera independiente para cada una de estas Soluciones Cartera. Esto implica que dicha entidad registrará diferentes anclas de confianza para cada una de sus Soluciones Cartera.

Encontrará más detalles sobre el proceso de notificación al Prestador de Cartera en el Tema 31.

6.2.3 Suspensión o retirada del Prestador de Cartera

En determinadas circunstancias, un Proveedor de la Lista de Confianza puede decidir suspender o retirar a un Proveedor de Carteras. Esto implica que el estado del Proveedor de Cartera en la respectiva Lista de Confianza cambiará a No Válido. Las condiciones para ello serán especificadas por cada Prestador de Lista de Confianza. Como consecuencia de este cambio de estado, los Proveedores de DIP, los Proveedores de

declaraciones y las Partes usuarias dejarán de confiar en los anclajes de confianza del Proveedor de Carteras y, por tanto, se negarán a interactuar con cualquier Unidad de Cartera proporcionada por dicho Proveedor de Carteras.

Cuando un Proveedor de Listas de Confianza retira a un Proveedor de Carteras, el Proveedor de Carteras revoca todas las WUAs válidas para todas las Unidades de Carteras, tal y como se describe en la Sección 6.6.3.12.

Si una entidad ha registrado varios Proveedores de Cartera, cada uno de los cuales ofrece una Solución de Cartera diferente, y uno de estos Proveedores de Cartera es suspendido o retirado, sólo se verá afectada la Solución de Cartera aplicable. Puede ocurrir que el motivo de la suspensión o retirada sea aplicable a todas las Soluciones de Cartera ofrecidas, en cuyo caso todos los Proveedores de Cartera registrados por esa entidad serán retirados o suspendidos por separado.

6.3 Confianza a lo largo del ciclo de vida de un Prestador de DIP o un Proveedor de Declaraciones

6.3.1 Ciclo de vida del Prestador de DIP o del Proveedor de declaraciones

En la sección 4.6.4 se presenta el ciclo de vida de un Prestador de DIP o de un Proveedor de Declaraciones:

1. Un Proveedor de DIP o un Proveedor de Declaraciones es registrado por un Proveedor de Listas de Confianza. Esto se trata en la sección 6.3.2.
2. En determinadas circunstancias, un Proveedor de Listas de Confianza puede decidir suspender o retirar a un Prestador de DIP o un Proveedor de Certificaciones registrado. Esto se trata en la sección 6.3.3.

6.3.2 DIP Registro y notificación del Prestador de servicios o del Proveedor de certificados

6.3.2.1 Introducción

La figura 11 muestra los Proveedores de DIP y los Proveedores de Certificados a la izquierda de la Unidad Cartera. A izquierda y por debajo, la figura también muestra que cada Proveedor de DIP y Proveedor de Certificados se registrará en una Lista de Proveedores de DIP de Confianza o en una Lista de Proveedores de Certificados de Confianza de su Estado miembro. Posteriormente, el Estado miembro notifica el Proveedor de DIP o el Proveedor de Certificados a la Comisión Europea.

Si los procesos de registro y notificación tienen éxito, ocurren principalmente dos cosas:

- El Prestador de DIP o el Proveedor de declaraciones recibe un certificado de acceso.
- Los anclajes de confianza del Prestador de DIP o del Prestador de declaraciones se incluyen en una Lista de confianza.

Estos dos procesos se analizan en las dos subsecciones siguientes.

6.3.2.2 Prestador de DIP o proveedor de declaraciones recibe un certificado de acceso

Cuando un Estado miembro registra un Proveedor de DIP o un Proveedor de Certificaciones, una Autoridad de Certificación de Acceso (AC) de Proveedor de DIP o una Autoridad de Certificación de Acceso de Proveedor de Certificaciones expide uno o más certificados de acceso al Proveedor de DIP o al Proveedor de Certificaciones. Un Prestador de DIP o un Proveedor de Certificados necesita un certificado de este tipo para autenticarse ante una Unidad Cartera cuando emite un DIP o una declaración para ella, tal como se describe en la sección 6.6.2.2. Un certificado de acceso de Proveedor de DIP indica que su sujeto es un Prestador de DIP. Del mismo modo, un certificado de acceso de proveedor de atestación indica que su sujeto es un Prestador de DEA, un Prestador de DEA-AAPP o un Prestador de DEA no cualificado.

Posteriormente, la autoridad de certificación de acceso se incluye en una lista de confianza de CA de acceso del Prestador de DIP o en una lista de confianza de CA de acceso del Prestador de atestación. Esta lista de confianza contiene al menos las anclas de confianza de la CA. Una Unidad Cartera puede utilizar estas anclas de confianza para verificar la autenticidad de un certificado de acceso de Proveedor de DIP o de Proveedor de atestación durante la emisión de un DIP o de una declaración. Para más información, consulte el Tema 31.

Tenga en cuenta que, en caso de que el sujeto sea un Prestador de servicios de certificación, el certificado de acceso no contiene más información sobre su autorización o registro para expedir declaraciones de un tipo específico, por ejemplo un Carné de Conducir Móvil (CCm) o un diploma. La autorización se tramita de la siguiente manera:

- En el caso de los Prestadores DEA y DEA-AAPP, no es necesaria ninguna autorización, ya que otros actores del ecosistema de Carteras IDUE confían en este tipo de Prestadores para que no emitan de forma fraudulenta declaraciones que no están legalmente autorizados a emitir. Esta confianza es

  La existencia de este tipo de Prestadores está justificada, ya que operan en un marco regulado y son objeto de auditorías periódicas.

- En el caso de los Prestadores de AEA no cualificados, esto es diferente, ya que no están regulados y pueden no ser completamente fiables. Sin medidas adicionales, un Prestador de CEA fraudulento puede ser técnicamente capaz de emitir tipos de CEA-Q, CEA-PuB o CEA que no está legalmente autorizado a emitir. Para , las Directrices de elaboración aplicables (véase el Tema 12) podrán definir mecanismos que permitan a una Unidad de Cartera, durante la emisión de una DEA, verificar que el Proveedor de DEA está autorizado o registrado para emitir el tipo de DEA que la Unidad de Cartera está solicitando. Las Partes usuarias (informadas) también podrán utilizar el mismo mecanismo durante la presentación de una DEA.

6.3.2.3 Los anclajes de confianza del Prestador de DIP o del Prestador de atestados se incluyen en una lista de confianza

Para un Prestador de DIP, un Prestador de DECA o un Prestador de DEA-AAPP, el registro y la notificación satisfactorios significan también que el Prestador se notifica a la Comisión Europea y que sus anclas de

confianza se incluyen en una lista de confianza. Las Partes usuarias pueden utilizar estas anclas de confianza para verificar la autenticidad de los DIP, las DEA y las DEA-PuB que obtienen de las Unidades Cartera.

Los Prestadores de DEA no cualificados no son incluidos en una Lista de Confianza por un Estado Miembro. Sin embargo, si una Parte usuaria (informada) solicita una DEA no cualificada a una Instancia de Cartera, debe saber cómo obtener el anclaje de confianza específico del dominio que necesita para verificar la firma sobre esa DEA. Para ayudar a ello, el Tema 12 recomienda que las Directrices de elaboración aplicables especifiquen los mecanismos que lo permitan. Este mecanismo puede ser similar al de las DECA, es decir, que los Prestadores de DEA no cualificados pertinentes y sus anclas de confianza se incluyan en una lista de confianza. Sin embargo, también pueden utilizarse otros métodos, e incluso si dicha lista de confianza existe, no tiene por qué cumplir los requisitos del Tema 31.

Encontrará más detalles sobre el proceso de notificación al Prestador de DIP o al Proveedor de Certificados, así como sobre la información registrada y publicada en la Lista de confianza de Prestadores de DIP o en la Lista de confianza de Proveedores de Certificados, en el Tema 31.

6.3.3 DIP Prestador o declaración Suspensión o retirada del prestador

En determinadas circunstancias, un Proveedor de Listas de Confianza podrá decidir suspender o retirar a un Prestador de DIP o un Proveedor de Certificados registrado. Las condiciones para ello serán especificadas por cada Prestador de Listas de Confianza.

La suspensión o retirada implica la revocación de los certificados de acceso del Prestador de DIP o del Prestador de atestados. En consecuencia, el Prestador de DIP o el Prestador de atestados ya no podrá emitir DIP ni declaraciones a las Unidades Cartera.

En el caso de un Proveedor de DIP, un Proveedor de DECA o un Proveedor de DEA-AAPP, la suspensión o retirada también implica que su estado en la respectiva Lista de confianza cambiará a No válido. En consecuencia, las Partes usuarias dejarán de confiar en los DIP o declaraciones emitidos por el Proveedor suspendido o retirado. En el caso de los Proveedores de DEA no cualificados, las Directrices de elaboración aplicables (véase el Tema 12) podrán definir mecanismos adicionales que garanticen que las Partes usuarias dejen de confiar en los anclajes de confianza de los Proveedores de DEA que hayan sido suspendidos o retirados.

Cuando un Proveedor de Listas de Confianza suspende o retira a un Proveedor de DIP o a un Proveedor de Certificados, el Proveedor de DIP o el Proveedor de Certificados revoca todos sus DIP o declaraciones, tal como se describe en la sección 6.6.3.7.

6.4 Confianza a lo largo del ciclo de vida de una Parte usuaria (informada)

6.4.1 Ciclo de vida de la Parte usuaria (informada)

La sección 4.6.6 presenta el ciclo de vida de una Parte usuaria (informada):

1. Una Parte usuaria (informada) es registrada por un Registrador en el Estado miembro en el que reside. El registro de Parte usuaria (informada) se trata en la Sección 6.4.2.
2. Bajo condiciones específicas, un Registrador puede decidir dar de baja a una Parte usuaria (informada) registrada. Esto se trata en la sección 6.4.3.

6.4.2 Registro de la Parte usuaria (informada)

La figura 11 muestra la Instancia de la Parte usuaria (informada) a la derecha de la Unidad Cartera. Una Instancia de Parte de Confianza es una combinación de hardware y software utilizada por una Parte usuaria (informada) para interactuar con una Unidad Cartera. Una Parte usuaria puede utilizar múltiples Instancias de Parte usuaria, especialmente en el caso de que las interacciones con la Unidad de Cartera tengan lugar en proximidad, por ejemplo, una agencia de control de fronteras en un aeropuerto que emplee múltiples líneas en las que los pasajeros que llegan puedan presentar su DIP.

La figura 11 también muestra la Parte usuaria (informada). Debajo, se muestra que cada Parte usuaria se registrará en un Registrador de Partes usuarias de su Estado miembro. Si el proceso de registro tiene éxito, el Registrador incluye a la Parte usuaria (informada) en su registro público.

Como resultado de un registro satisfactorio,

- el Registrador expide un certificado de registro a la Parte usuaria (informada). La finalidad del certificado de registro se describe en la sección 6.6.3.3.
- una Autoridad de Certificación de Acceso (CA) de Instancia de Parte Confiable asociada con el Registrador emite un certificado de acceso a cada Instancia de Parte Confiable de la Parte Confiable. Una Instancia de Parte usuaria necesita dicho certificado para autenticarse ante Unidades Cartera cuando solicita la presentación de atributos, tal y como se describe en la Sección 6.6.3.2.

Posteriormente, un Prestador de Listas de Confianza en cada Estado miembro crea una Lista de Confianza de CA de Acceso a Instancia de Parte usuaria que contiene la(s) ancla(s) de confianza de todas las CA de Acceso a Instancia de Parte usuaria asociadas. Una Unidad Cartera puede utilizar estas anclas de confianza para verificar la autenticidad de los certificados de acceso a la Instancia de la Parte usuaria. El Prestador de la Lista de Confianza firma y publica la Lista de Confianza de la CA de Acceso a la Instancia de la Parte usuaria y pone la URL de la Lista de Confianza a disposición de una infraestructura de confianza común mantenida por la Comisión, la denominada Lista de Listas de Confianza. Utilizando la infraestructura común, cualquier entidad del ecosistema Cartera IDUE podrá encontrar todas las listas de confianza del ecosistema.

Encontrará más información sobre el proceso de registro de Parte usuaria (informada) en el Tema 27.

6.4.3 Baja de la Parte usuaria (informada)

Bajo específicas, un Registrador puede decidir dar de baja a una Parte usuaria (informada) registrada. Las condiciones para ello serán especificadas por cada Registrador.

La baja implica la revocación de todos los certificados válidos de acceso a la Instancia de la Parte usuaria por parte de la CA de acceso correspondiente, de forma que la Parte usuaria ya no puede interactuar con las Unidades de Cartera.

6.5 Confianza a lo largo del ciclo de vida de una Unidad Cartera

6.5.1 Ciclo de vida de la unidad Cartera

En el apartado 4.6.3 se ha presentado el ciclo de vida de una Unidad Cartera:

1. La Instancia Cartera que es parte de la Unidad Cartera es instalada en un dispositivo por un Usuario. Las relaciones de confianza necesarias para la instalación se tratan en la Sección 6.5.2 más adelante.
2. A continuación, la Unidad Cartera es activada por el Prestador de Carteras y el Usuario y entra en funcionamiento. Los objetivos y las relaciones de confianza necesarias para la activación se tratan en la Sección 6.5.3.
3. Una vez en estado **Operativo** o **Válido**, la Unidad Cartera es gestionada por el Usuario y el Prestador de Carteras. Esta gestión incluye al menos la revocación de la Unidad Cartera cuando sea necesario. Esto se discute en la Sección 6.5.4. La gestión también incluirá actualizaciones periódicas de la aplicación Instancia Cartera para garantizar su seguridad y funcionalidad continuas. Sin embargo, esto no se define con más detalle en este capítulo.
4. El Usuario puede desinstalar la Instancia Cartera; ver Sección 6.5.5.

6.5.2 Instalación de la Instancia Cartera

6.5.2.1 Relaciones de confianza necesarias

El ciclo de vida de una Unidad Cartera comienza cuando un Usuario decide instalar una aplicación Instancia Cartera en su dispositivo. Esta aplicación en una instancia de una Solución Cartera, que es proporcionada al Usuario por un Prestador de Carteras.

Al descargar e instalar la Instancia Cartera, se establecen las siguientes relaciones de confianza:

1. En nombre del Usuario, el sistema operativo del dispositivo del Usuario y la tienda de aplicaciones pertinente verifican que la Instancia de Cartera (es decir, la aplicación que el Usuario está instalando) es genuina y auténtica y no contiene ningún malware u otras amenazas.
2. El Usuario verifica que puede obtener los DIP que necesita en una instancia de esta Solución Cartera. Si el Prestador de DIP pertinente no admite Cartera el Usuario no podrá utilizar la Unidad Cartera para obtener dicho(s) DIP(s).

En las dos secciones siguientes se analizan estas relaciones de confianza.

6.5.2.2 Se verifica la autenticidad de la solución Cartera

Para garantizar que el Usuario pueda confiar en la Solución Cartera, los Prestadores de Carteras preferiblemente hacen que sus Soluciones Cartera certificadas estén disponibles para su instalación a través de la tienda oficial de aplicaciones del sistema operativo correspondiente (por ejemplo, Android, iOS). Esto permite al sistema operativo del dispositivo realizar las comprobaciones pertinentes sobre la autenticidad de la aplicación. También permite a los usuarios utilizar el mismo canal conocido para obtener una instancia de Cartera que utilizan para obtener otras aplicaciones. último, evita una situación en la que un usuario deba permitir la carga lateral de aplicaciones, lo que aumentaría el riesgo de instalar involuntariamente aplicaciones maliciosas.

Si un Prestador de Carteras pone a disposición su Solución Cartera para su instalación a través de medios distintos de la tienda oficial de aplicaciones del SO, implementa un mecanismo que permite al Usuario verificar la autenticidad de la Unidad Cartera. Además, el Prestador de Carteras proporciona instrucciones claras al Usuario sobre cómo instalar la Unidad Cartera, incluyendo:

- instrucciones sobre cómo verificar la autenticidad de la Instancia Cartera que se va a instalar. Esto puede hacerse, por ejemplo, comparando el valor hash de la aplicación descargada por el Usuario con un valor hash publicado por el Prestador de Carteras.
- instrucciones para evitar cualquier limitación del sistema operativo en cuanto a la carga lateral de aplicaciones, si procede, y garantizar que estas limitaciones se restauren una vez instalada la Instancia de Cartera.

Nota: El [Reglamento Europeo de Identidad Digital] no excluye la posibilidad de que una Instancia de Cartera pueda instalarse en un dispositivo que no sea móvil, por ejemplo un servidor. Los requisitos anteriores también se aplican para la instalación de una Instancia de Cartera en un dispositivo de Usuario que no sea un dispositivo móvil, y para el que puede no existir una tienda de aplicaciones oficial del sistema operativo.

6.5.2.3 El usuario valida que la solución Cartera es utilizable con el DIP correspondiente

Un Usuario instala una Unidad Cartera porque desea obtener y utilizar uno o más DIP. Sin embargo, los Proveedores de DIP no están obligados a dar soporte a todas las Soluciones Cartera del ecosistema Cartera IDUE. Soporte" significa aquí que el Proveedor de DIP está dispuesto a emitir un DIP a una instancia de una determinada Solución de Cartera a petición del Usuario. En cambio, un Prestador de DIP puede optar por dar soporte a una única Solución Cartera o a un número limitado de Soluciones Cartera. Por lo tanto, cada Proveedor de DIP publicará una lista de las Soluciones Cartera que soporta, de forma que un Usuario que quiera solicitar un DIP a ese Proveedor de DIP sepa qué Unidad Cartera debe instalar. Esta lista podría publicarse, por ejemplo, en el sitio web del Prestador de DIP.

Por el contrario, no es necesario que una Solución Cartera admita a todos los Proveedores de DIP, entendiéndose por "admitir" la capacidad de solicitar la emisión de un DIP a un Proveedor de DIP. Cada Proveedor de Carteras, antes o durante la instalación de una Instancia de Cartera, comunicará al Usuario qué Proveedores de DIP son compatibles con esta Solución de Cartera.

En el caso de los DECA, DEB-AAPP y DEA-AAPP no cualificados, la situación es diferente. Los Prestadores de este tipo de certificados admitirán todas las Soluciones Cartera y no podrán discriminar entre ellas a la hora de tramitar una solicitud de emisión de un certificado. A la inversa, una Solución Cartera admite todos los Proveedores de Certificados, y no puede discriminar entre diferentes Proveedores de Certificados al solicitar la emisión de un certificado a petición del Usuario.

6.5.3 Activación de la Unidad Cartera

6.5.3.1 Introducción

Tras la instalación de Instancia Cartera, la nueva Unidad Cartera (que incluye dicha Instancia Cartera) se pondrá en contacto con el Prestador de Carteras para iniciar el proceso de activación. Para que la activación de la Instancia Cartera IDUE se realice correctamente, se establecen las siguientes relaciones de confianza:

1. La Instancia de Cartera IDUE autentica al Prestador de Cartera IDUE, lo que significa que la instancia está segura de que está tratando con el Prestador de Cartera genuino que la proporcionó al Usuario.
2. El Prestador de Carteras IDUE autentica la Instancia de Cartera IDUE. Esto significa que el Prestador de Carteras IDUE está seguro de que la instancia es realmente una instancia real de su Solución de Carteras IDUE, y no una aplicación falsa.

Ambas relaciones de confianza son responsabilidad del Prestador de Cartera. El ARF no especifica cómo pueden satisfacerse estas relaciones de confianza.

Durante el proceso de activación, ocurren al menos los siguientes pasos:

1. El Prestador de Cartera solicita datos sobre el dispositivo del Usuario a la Instancia de Cartera. 2. El Prestador de Carteras solicita al Usuario que configure al menos un mecanismo de autenticación de Usuario.
3. El Prestador de Cartera emite una o más Declaraciones de Unidad de Cartera a la Unidad de Cartera.
4. El Prestador de Cartera crea una cuenta de Usuario para el

Usuario. Estos pasos se describen en las secciones siguientes.

6.5.3.2 El Prestador de Cartera solicita datos sobre el dispositivo del Usuario a la Instancia de Cartera

La Instancia Cartera se conecta al Proveedor de Carteras para ser activada. A continuación, el Proveedor de Cartera solicita datos sobre el dispositivo del Usuario a la Instancia de Cartera. Estos datos pueden incluir las tecnologías de comunicación soportadas por el dispositivo y las características de los WSCD disponibles en el dispositivo para almacenar de forma segura claves criptográficas y datos asociados a la propia Instancia Cartera y a las declaraciones de dicha Instancia Cartera.

Notas:

- Como se explica en la sección 4.5, un WSCD puede estar integrado directamente en el dispositivo del usuario. Ejemplos de ello son una e-SIM, una UICC, un elemento seguro integrado o un hardware seguro nativo accesible a través del sistema operativo del dispositivo. Si es así, la Instancia de Cartera descubrirá la presencia de tal WSCD durante la activación y comunicará las características del WSCD al Prestador de Cartera. En algunos casos, el Proveedor de Cartera desplegará posteriormente una WSCA en el WSCD para facilitar la comunicación entre la Instancia de Cartera y el WSCD.
- A veces, el dispositivo del usuario no contiene un WSCD, o el WSCD no tiene la postura de seguridad necesaria para permitir que la Unidad Cartera sea un medio de identidad en LoA "alto". En tal caso, el Proveedor de Cartera garantiza que la Unidad de Cartera tenga acceso a un HSM remoto operado por el Proveedor de Cartera.

6.5.3.3 El Prestador de Carteras solicita al Usuario que configure al menos un mecanismo de autenticación de Usuario.

La autenticación del usuario tendrá lugar en varios momentos cuando un usuario utilice su Unidad Cartera:

1. Cuando el Usuario abre la Instancia Cartera. Esto es necesario para evitar que cualquier persona, excepto el Usuario, acceda a la Instancia Cartera e inspeccione las declaraciones y valores de atributos del Usuario. Estos datos son personales y pueden ser sensibles.
2. Cuando (o antes) la Unidad Cartera solicita al Usuario su aprobación para presentar algunos atributos a una Parte usuaria (informada), véase el apartado 6.6.3.5.

La autenticación del usuario para la apertura de la Instancia de Cartera anterior puede ser realizada por la Instancia de Cartera o por un WSCD. En este último , se trata del mismo mecanismo empleado antes de la presentación de cualquier atributo, véase más adelante. En el primer caso, el mecanismo es específico de la Unidad Cartera, lo que significa que es independiente de cualquier mecanismo general de autenticación de Usuario utilizado por el dispositivo de Usuario, como una pantalla de bloqueo.

La autenticación del usuario antes de presentar atributos siempre la realiza la WSCA. Significa que el Usuario da permiso a la WSCA para utilizar las claves criptográficas pertenecientes a la Unidad Cartera y al DIP o declaración para realizar las operaciones criptográficas necesarias para presentar dicho DIP o declaración. Por ello, en este caso es siempre la WSCD la que realiza la autenticación del Usuario.

Durante la activación de la Unidad Cartera, dependiendo de la elección realizada por el Proveedor de Carteras de combinar o no los dos mecanismos de autenticación del Usuario, el Proveedor de Carteras solicitará al Usuario que configure uno o dos mecanismos de autenticación.

Tenga en cuenta que, como se indica en el primer punto del apartado 6.6.3.9, los mecanismos de autenticación de usuario implementados en el WSCD también pueden desempeñar un papel a la hora de garantizar la vinculación del usuario. La vinculación del usuario permite a la Parte usuaria confiar en que la persona que presenta un DIP o una declaración es realmente el sujeto de dicho DIP o declaración.

6.5.3.4 Prestador de Cartera emite una o más Declaraciones de Unidad de Cartera a la Unidad de Cartera

Durante la activación de una Unidad Cartera, el Prestador de Cartera emite una o más Declaraciones de Unidad Cartera a la Unidad Cartera. La Declaración de Unidad Cartera (WUA) se describe en el Tema 9. También puede encontrar más información sobre la WUA en el documento de debate del tema C.

Una WUA tiene tres objetivos principales:

- Describe las capacidades y propiedades de la Unidad Cartera, incluida la Instancia Cartera, el dispositivo de Usuario y el o los WSCD. Esto permite a un Proveedor de DIP o a un Proveedor de Declaraciones verificar que la Unidad Cartera cumple los requisitos del Proveedor y, por tanto, es apta para recibir un DIP o una declaración del Proveedor. Para garantizar la privacidad del usuario, la Unidad Cartera sólo presenta sus capacidades y propiedades a los Proveedores de DIP y a los Proveedores de Certificados, pero no a las Partes usuarias (informadas). Esto se debe a que los Proveedores de DIP y los Proveedores de Declaraciones tienen una razón comercial válida para conocer estas propiedades, mientras que las Partes usuarias no. El documento de debate sobre el tema C se refiere a ellos como "caso de uso 1" (Partes usuarias) y "caso de uso 2" (Proveedores de DIP y Proveedores de certificados).
- Además, la WUA contiene una clave pública WUA. Durante la emisión de un DIP o una declaración (véase la sección 6.6.2.3), un Proveedor de DIP o un Proveedor de Declaraciones puede utilizar esta clave pública para verificar que la Unidad Cartera está en posesión de la clave privada correspondiente. Además, en ese , la Unidad Cartera enviará otra clave pública al Proveedor de DIP o al Proveedor de atestación. El Prestador incluirá esta clave pública en el DIP o la declaración emitidos. El Prestador de DIP o el Prestador de Atestados podrá verificar opcionalmente que la clave privada perteneciente a esta clave pública está protegida por el mismo WSCD que la clave privada perteneciente a la clave pública de la Unidad Monedero, si así lo admite el WSCD. De este modo, el Prestador de DIP o el Prestador de Declaraciones pueden confiar en esta nueva clave pública. Nótese que el soporte de dicha prueba no es obligatorio en esta versión del ARF, ya que aún no se ha especificado ningún mecanismo, y mucho menos que esto sea ampliamente soportado por los WSCD disponibles.

- Por último, si un DUA es válido durante 24 horas o más, contiene información que permite a un Proveedor de DIP, a un Proveedor de declaraciones o a una Parte usuaria verificar que el Proveedor de Cartera

  no revocó la declaración de la Unidad Cartera y, por tanto, la propia Unidad Cartera. La WUA y los mecanismos de revocación de Unidades Cartera se describen en el Tema 38.

El formato detallado de la WUA se especificará en una especificación técnica. Puede haber diferencias en el formato de los WUA adecuados para el caso de uso 1 y los del caso de uso 2. En concreto, las WUA destinadas a Partes usuarias (informadas) probablemente se ajustarán a [ISO/IEC 18013-5] o [SD-JWT VC], para evitar requisitos adicionales a las Partes usuarias (informadas) y a las Unidades de Cartera. En el caso de las WUA

destinadas a Prestadores de DIP o Prestadores de declaraciones, no existe tal limitación, y el formato de éstas puede ser más sencillo.

En cuanto al periodo de validez de la WUA, un requisito importante del artículo 5 de la [CIR 2024/2977] es que un Proveedor de DIP debe revocar un DIP cuando se revoque la Unidad Cartera a la que se emitió dicho DIP. Esto implica que un Proveedor de DIP, durante todo el periodo de validez del DIP, debe ser capaz de comprobar regularmente si el Proveedor de Cartera revocó la WUA que el Proveedor de DIP obtuvo de la Unidad de Cartera durante la emisión del DIP. Para poder hacerlo, el período de validez de las WUA destinadas a los Prestadores de DIP será largo, quizá tanto como la vida útil prevista de la Unidad Cartera. Además, el periodo de validez de un DIP no puede superar el final de la validez la WUA recibida por el Prestador de DIP durante la emisión.

Las responsabilidades del Proveedor de Carteras en relación con la emisión de una WUA son similares a las de un Proveedor de DIP o un Proveedor de Certificados en relación con la emisión de un DIP o un certificado. Esto significa que después de la emisión inicial de un WUA durante la activación, el Proveedor de Carteras gestionará el WUA y emitirá nuevos WUAs a la Unidad de Cartera según sea necesario, durante la vida útil de la Unidad de Cartera. En particular, el Prestador de Carteras garantizará que se minimice el riesgo de que Partes usuarias malintencionadas vinculen múltiples presentaciones de la misma WUA, con el objetivo de rastrear al usuario. Por ejemplo, el Proveedor de Carteras puede configurar la Unidad de Cartera de forma que cada Declaración de Unidad de Cartera se presente como máximo a un Proveedor de DIP, Proveedor de Declaración o Parte usuaria (informada). Este tipo de WUA se denomina declaración "única" (véase la sección 7.4.3.5).

6.5.3.5 El Prestador de Carteras crea una cuenta de Usuario para el Usuario

El Usuario necesita una cuenta de Usuario en el Prestador de Carteras para poder solicitar la revocación de su Unidad de Cartera en caso de robo o pérdida. El Proveedor de Carteras asocia la Unidad Cartera a la cuenta de Usuario. El Proveedor de Carteras registra uno o más métodos de autenticación de Usuario basados en backend que el Proveedor de Carteras utilizará para autenticar al . Tenga en cuenta que:

- El Prestador de Carteras no necesita conocer ningún atributo del mundo real del Usuario. El sitio
  El Usuario puede utilizar un seudónimo para registrarse, por ejemplo una dirección de correo electrónico. Si el Prestador de Carteras desea solicitar atributos adicionales del Usuario, por ejemplo para poder prestarle servicios adicionales, es libre de hacerlo si el Usuario da su consentimiento.
- En cualquier caso, los datos de Usuario registrados por el Prestador de Carteras no se incluirán en la WUA. Son de uso del Prestador de Carteras.

6.5.4 Gestión de la Unidad Cartera

A partir de la activación de la Unidad Cartera y hasta que la Instancia Cartera sea desinstalada por el Usuario, una Unidad Cartera es gestionada por el Usuario y el Prestador de Carteras. El Prestador de Carteras es responsable como mínimo de:

- realizar la instalación de una nueva versión de la Solución Cartera según sea necesario.
- actualizar las WUA según sea necesario; véase el Tema 9.
- revocar la Unidad Cartera en caso de que su seguridad se vea comprometida; véase el Tema 38.

El Usuario podrá solicitar al Prestador de Carteras la revocación de la Unidad de Cartera al menos en de pérdida o robo del dispositivo del Usuario. Véase el Tema 38.

Si la Unidad de Cartera contiene un DIP, el Proveedor de DIP puede solicitar al Proveedor de Carteras que revoque la Unidad de Cartera en caso de que la persona física usuaria de la Unidad de Cartera haya fallecido o la persona jurídica usuaria de la Unidad de Cartera haya cesado sus operaciones. Véase el Tema 38.

Por último, la Unidad Cartera admite procedimientos para realizar copias de seguridad y restaurar las declaraciones que contiene, o para migrar estas declaraciones a una Solución Cartera diferente. Consulte los Temas 33 y 34 respectivamente.

Para permitir la gestión de la Unidad Cartera, se establecen las siguientes relaciones de confianza:

1. Al contactar con el Prestador de Carteras, por ejemplo para solicitar la revocación de la Unidad Cartera, el Usuario autentica al Prestador de Carteras. Esto significa que el Usuario está seguro de que está visitando el sitio web o el portal de usuario del auténtico Proveedor de Carteras responsable de la Unidad de Cartera del Usuario, y no un sitio web o portal falsificado. Este riesgo puede mitigarse en parte utilizando mecanismos estándar como la autenticación de servidor TLS. Sin embargo, el usuario también tendrá que estar alerta, al igual que con cualquier sitio web en Internet.
2. Al ser contactado por un Usuario, el Proveedor de Carteras autentifica al . Esto significa que el Prestador de Carteras está seguro de que el Usuario es efectivamente el Usuario que estaba asociado a

   la Unidad Cartera durante la activación. Para ello, el Prestador de Carteras utiliza los métodos de autenticación establecidos en la cuenta del Usuario durante la activación, véase el apartado 6.5.3. 3. Cuando la Unidad de Cartera y el Proveedor de Cartera establecen un canal de comunicación, la Unidad de Cartera autentica al Proveedor de Cartera, lo que significa que la Unidad de Cartera está segura de que está tratando con el Proveedor de Cartera genuino. Del mismo modo, el Proveedor de Carteras autentica a la Unidad de Carteras. Esto significa que el Proveedor de Carteras está seguro de que la Instancia de Cartera IDUE es realmente una instancia real de su Solución de Cartera, y no una aplicación falsa. Esto será garantizado por el Prestador de Carteras. El ARF no especifica cómo pueden satisfacerse estas relaciones de confianza.
4. Cuando un Proveedor de DIP se pone en contacto con él para solicitar la revocación de la Unidad Cartera, el Proveedor de Carteras autentica al Proveedor de DIP. La sección 6.6.2.2 describe cómo una Unidad Cartera puede hacer esto durante la emisión de DIP; un Proveedor Cartera puede utilizar el mismo mecanismo.
5. Para identificar la Unidad Cartera que va a ser revocada, el Prestador de DIP utiliza un identificador de Unidad Cartera proporcionado por la Unidad Cartera en la WUA durante la emisión del DIP; véase el Tema 9.

6.5.5 Desinstalación de la Instancia Cartera

No se requieren relaciones de confianza para la desinstalación de la Instancia Cartera; cualquiera que pueda acceder al dispositivo del Usuario podrá hacerlo.

Si el Usuario desinstala la Instancia de Cartera, la Instancia de Cartera garantiza que la(s) WSCA(s) asociada(s) elimina(n) todos los datos sensibles y claves criptográficas relacionados con la Unidad de Cartera y con todos los DIP y declaraciones de la Unidad de Cartera.

Si soporta la API de Credenciales Digitales, ver Sección 4.4.3, la Instancia de Cartera también revela el hecho de que está desinstalada al marco de la API de Credenciales Digitales.

6.6 Confianza a lo largo del ciclo de vida de un DIP o una declaración

6.6.1 DIP o ciclo de vida de la declaración

En la sección 4.6.5 anterior se ha presentado el ciclo de vida de un DIP o declaración dentro de una Unidad Cartera:

1. Utilizando su Unidad Cartera, el Usuario solicita la emisión de un DIP o una declaración a un Proveedor de DIP o a un Proveedor de Declaraciones. Las relaciones de confianza necesarias para la emisión se describen en la sección 6.6.2.
2. Una vez emitido el DIP o la declaración en la Unidad Cartera, el Usuario puede presentar atributos de la misma a una Instancia Parte usuaria, según decida el Usuario y en función de

   autenticación correcta de la Parte usuaria (informada). Las relaciones de confianza necesarias para el envío previo de DIP y declaraciones, incluida la aprobación del usuario y la autenticación de la Parte usuaria (informada), se tratan en la sección 6.6.3.
3. En lugar de presentar atributos a una Parte usuaria (informada), un Usuario también puede presentarlos a otro Usuario, lo que significa que su Unidad Cartera está interactuando con otra Unidad Cartera. Esto se discute brevemente en la Sección 6.6.4.
4. El Prestador del DIP o el Prestador del certificado sigue siendo responsable de la gestión del DIP o de la declaración a lo largo de su vida útil. La gestión puede incluir la reemisión del DIP o de la declaración con los mismos valores de atributo o con valores diferentes. El Prestador también puede revocar el DIP o la declaración, posiblemente a petición del Usuario. La gestión de los DIP y las declaraciones se trata en la sección 6.6.5.
5. Por último, en el apartado 6.6.6 se explica qué ocurre si un Usuario decide eliminar un DIP o una declaración de su Unidad Cartera.

6.6.2 Expedición del DIP o de la declaración

6.6.2.1 Relaciones de confianza necesarias

El ciclo de vida de un DIP o de una declaración comienza cuando un Usuario, utilizando su Unidad Cartera, solicita a un Proveedor de DIP o a un Proveedor de Declaraciones que emita el DIP o la declaración para su Unidad Cartera. Durante la emisión se establecen las siguientes relaciones de confianza:

1. La Unidad Cartera autentica al Proveedor de DIP o al Proveedor de Certificados utilizando el certificado de acceso mencionado en la Sección 6.3. Esto garantiza que el Usuario puede confiar en que el DIP o la declaración que está a punto de recibir ha sido emitido por un Prestador de DIP o un Prestador de Declaraciones autenticado, respectivamente. Véase el apartado 6.6.2.2, en el que se describe cómo hacerlo.
2. El Prestador de DIP o Prestador de atestados autentica al Usuario, lo que significa que el Prestador está seguro de la identidad del Usuario. Esto es necesario para poder determinar los valores de los atributos que el Prestador va a . Por ejemplo, un Prestador de DIP necesita autenticar al Usuario para asegurarse de que proporciona un DIP que contiene el apellido y la fecha de correctos. El método mediante el cual el Proveedor de DIP o el Proveedor de atestados lleva a cabo la identificación y autenticación del Usuario queda fuera ámbito del ARF, ya que estos procesos son específicos de cada Proveedor de DIP o Proveedor de atestados. No obstante, satisfarán los requisitos del Nivel de Aseguramiento exigido para el DIP o la declaración expedidos.
3. El Prestador de DIP o el Prestador de Declaraciones autentica y valida la Unidad de Cartera, véase el apartado 6.6.2.3 siguiente.
4. El Proveedor de DIP o el Proveedor de Declaraciones verifica que el Proveedor de Carteras no ha revocado la Unidad de Cartera. Esto se describe en la sección 6.6.2.4.
5. Una vez emitido el DIP o la declaración a la Unidad Cartera, ésta verifica la autenticidad del DIP o de la declaración; véase el apartado 6.6.2.5.
6. El usuario activará un DIP antes de poder ; véase el apartado 6.6.2.6.
7. Si una declaración contiene una política de divulgación incrustada, la Unidad Cartera recupera la política y la almacena localmente, para poder aplicarla en caso de que una Parte usuaria (informada) solicite atributos de la declaración. Véase la sección 6.6.2.7.

En el Tema 10/23 .se incluyen requisitos más detallados para el proceso de expedición de DIP y declaraciones, por ejemplo, en relación con el protocolo de expedición

6.6.2.2 La Unidad Cartera autentica al Prestador de DIP o al Prestador de Declaraciones

Como se muestra en la Figura 11, una Unidad Cartera descarga la(s) Lista(s) de Confianza de la AC de Acceso del Prestador de DIP que necesita del (de los) Proveedor(es) de Listas de Confianza pertinente(s), posiblemente después de haberlas localizado a través de la infraestructura de confianza común de la

Comisión. También descargará todas las listas confianza de las AC de acceso de los Prestadores de declaración. Para más información sobre estas listas de confianza, véase la sección 6.3.2.

Nota: No es obligatorio que cada Unidad Cartera posea todas las Listas de Confianza de CA de Proveedores de DIP, si existen múltiples. Los Prestadores de Cartera elegirán a qué Listas de Confianza deben suscribirse, por ejemplo, en función del Estado o Estados Miembros en los que operen. Sin embargo, es obligatorio poseer todas las listas de confianza de CA de acceso de proveedores de declaración, ya que las unidades de cartera deben admitir a todos los proveedores de DEA y DEA-AAPP del ecosistema de Carteras IDUE.

Para iniciar el proceso de solicitud de un DIP o una declaración, el Usuario indica a la Unidad Cartera que se ponga en contacto con el Proveedor de DIP o el Proveedor de Declaraciones. Para ello, el usuario puede, por ejemplo, utilizar la unidad Cartera para escanear un código QR o tocar una etiqueta NFC. Tenga en cuenta que no está previsto ningún mecanismo centralizado de descubrimiento de servicios para la emisión de DIP o declaraciones.

Antes de solicitar la emisión de un DIP o una declaración, la Unidad Cartera autentica al Proveedor de DIP o al Proveedor de Declaraciones. Para ello, la Unidad Cartera verifica el certificado de acceso que le presenta el Proveedor de DIP o el Proveedor de Atestados en sus metadatos de Emisor según [OpenID4VCI]. La Unidad Cartera comprueba que el certificado de acceso indica que su sujeto es un Prestador de DIP o un Prestador de Atestados. La Unidad Cartera también verifica que el certificado de acceso

es auténtico, que es válido en el momento de la validación y que el emisor del certificado es una CA que figura en la lista de confianza de CA de acceso del Prestador de DIP o del Prestador de declaración.

6.6.2.3 El Prestador de DIP o el Prestador de Declaraciones valida la Unidad Cartera

6.6.2.3.1 Verifica la autenticidad de la Unidad Cartera

Como se muestra en la figura 11, un Prestador de DIP o un Prestador de Declaraciones descarga la(s) Lista(s) de Confianza del Prestador de Carteras que necesita del (de los) Prestador(es) de Listas de Confianza pertinente(s), posiblemente después de haberlas localizado a través de la infraestructura de confianza común de la Comisión.

Tenga en cuenta que para los Prestadores de DIP no es obligatorio poseer todas las Listas de Confianza de Prestadores de Cartera, si existen múltiples. Esto se debe a que no es obligatorio que un Prestador de DIP acepte todas las Soluciones de Cartera certificadas en el ecosistema de Carteras IDUE. Cada Prestador de DIP elegirá a qué Listas de Confianza debe suscribirse. En el caso de los Prestadores de servicios de certificación, es diferente: deben aceptar todas las Soluciones de Cartera y, por lo tanto, deben poseer todas las Listas de Confianza de Prestadores de Cartera.

La sección 6.5.3 anterior describe que un Proveedor de Cartera, durante la activación de una Unidad de Cartera, emite una o más Declaraciones de Unidad de Cartera (WUA) a la Unidad de Cartera. Cuando la Unidad Cartera envía una solicitud de DIP o de declaración a un Proveedor de DIP o a un Proveedor de Declaraciones, incluye la WUA en la solicitud. El Proveedor de DIP o el Proveedor de Atestados verifica la firma sobre la WUA, utilizando el ancla de confianza del Proveedor de Carteras obtenida de la Lista de Confianza. A continuación, el Prestador de DIP o el Prestador de atestados verifica que la Unidad Cartera

posee la clave privada perteneciente a la clave pública del WUA. Esto demuestra que la Unidad Cartera es auténtica y que la proporciona un Prestador de Carteras de confianza. Para más detalles, véase el Tema 9.

6.6.2.3.2Opcionalmente, verifica que la Unidad Cartera del Usuario soporta todas las funciones requeridas.

La WUA describe las características relevantes de la Instancia Cartera, así como del dispositivo en el que está instalada. En función de sus necesidades, los Prestadores de DIP o los Proveedores de Certificaciones pueden comprobar opcionalmente que la Instancia de Cartera del Usuario es compatible con todas las funciones que necesitan. Por ejemplo, para algunos Prestadores de DIP o Proveedores de Certificaciones puede ser relevante saber si la Unidad Cartera admite la presentación de la declaración en flujos de proximidad utilizando NFC.

6.6.2.3.3Opcionalmente, valida las propiedades del WSCD

La WUA describe las certificaciones y otras propiedades relevantes del WSCD, decir, el dispositivo criptográfico seguro incluido en la Unidad Cartera para almacenar y gestionar claves criptográficas. El nivel de seguridad del WSCD es un factor determinante para el Nivel de Aseguramiento (LoA) global de la Unidad Cartera. Para obtener un DIP, la Unidad Cartera y el WSCD cumplirán lo siguiente

los requisitos de LoA Alto. Para otras declaraciones, se necesitará una LoA Alta o Sustancial, dependiendo de los requisitos del Prestador del Certificado.

6.6.2.3.4Verifica que la clave DIP o la clave de declaración está protegida por el WSCD

Conocer las propiedades del WSCD no es muy útil si el Prestador de DIP o el Proveedor de Certificados no puede estar seguro de que la clave privada de su nuevo DIP o declaración está realmente protegida por ese WSCD. El tema 9 describe cómo el Prestador de DIP o el Prestador de Certificados pueden obtener una prueba de que el WSCD descrito en la WUA protege tanto la clave privada de la WUA como la clave privada del nuevo DIP o declaración.

6.6.2.4 El Prestador de DIP o el Prestador de declaración verifica que no se ha revocado la UTA

La sección 6.5.3 anterior describe que un Proveedor de Cartera, durante la activación de una Unidad de Cartera, emite una o más Declaraciones de Unidad de Cartera (WUA) a la Unidad de Cartera. Si un WUA es válido durante más de 24 horas, contiene información de revocación. Durante la vida útil de la Unidad Cartera, el Prestador de Carteras verifica periódicamente que la seguridad de la Unidad Cartera no ha sido violada o comprometida. Si la Unidad de Cartera deja de ser segura, el Prestador de Carteras revoca cualquiera de sus WUAs que tenga un periodo de validez restante de 24 horas o más. Si el Proveedor de Carteras utiliza WUAs con un periodo de validez inferior a 24 , dejará de emitir nuevas WUAs para una Unidad de Cartera que ya no sea segura. De este modo, la WUA permite a los Proveedores de DIP, a los Proveedores de declaraciones y a las Partes usuarias verificar que la Unidad de Cartera no está revocada.

El Tema 38 describe la revocación de la Unidad Cartera con más detalle.

Una vez realizadas todas las comprobaciones, el Prestador de DIP o el Prestador de Certificaciones emitirá el DIP o la declaración a la Unidad Cartera.

6.6.2.5 La Unidad Cartera verifica el DIP o la declaración

Después de que la Unidad Cartera reciba el DIP o la declaración, procederá a lo siguiente

- comprobar que el DIP o la declaración que ha recibido coinciden con la solicitud.
- verificar la firma del DIP o la declaración, utilizando el anclaje de confianza adecuado, del mismo modo que se describe para una Instancia de Parte usuaria en la sección 6.6.3.6.
- mostrar el contenido (es decir, los valores de los atributos) del nuevo DIP o declaración al Usuario y solicitar la aprobación del Usuario para almacenar el nuevo DIP o declaración. Al solicitar la aprobación, la Unidad Cartera muestra el contenido del DIP o declaración al Usuario. La Unidad Cartera también informa al Usuario de la identidad del Prestador del DIP o de la declaración.

  Prestador, utilizando la información del asunto del certificado de acceso del Prestador de DIP o del Prestador de declaración.

Si una de estas verificaciones falla, la Unidad Cartera borrará el DIP o la declaración e informará al Usuario de que la emisión no se ha realizado correctamente. En caso contrario, la Unidad Cartera almacenará el DIP o la declaración e informará al Usuario de que la emisión se ha realizado correctamente. Si es compatible con la API de credenciales digitales, la sección 4.4.3véase , la Unidad Cartera también revelará el hecho de que contiene el nuevo DIP o atestación al marco de la API de credenciales digitales.

6.6.2.6 El usuario activa el DIP

Como se documenta en el Tema 9, para alcanzar un Nivel de Aseguramiento (LoA) "alto", el Reglamento de (UE) 2015/1502 de la Comisión requiere que se implemente un proceso de activación para verificar que un DIP fue efectivamente entregado en posesión de la persona a la que pertenece.

Sin embargo, en realidad no es necesario ningún paso adicional en el proceso de emisión para garantizarlo. Esto se debe a que el Usuario siempre inicia el proceso de emisión desde la Unidad Cartera en la que desea que el Proveedor de DIP emita el nuevo DIP. El Prestador de DIP establece un canal de comunicación seguro hacia esta Unidad Cartera, utilizando el flujo especificado en [OpenID4VCI]. Además, el Usuario utiliza un medio eID en LoA High para autenticarse hacia el Proveedor de DIP. Este proceso garantiza que el nuevo DIP sólo puede terminar en el dispositivo utilizado por el sujeto del DIP.

Tenga en cuenta que la activación sólo se requiere formalmente para DIP, ya que el [Reglamento Europeo de Identidad Digital] sólo exige que los DIP se expidan en LoA "alto". No obstante, lo anterior se aplica a los DECA, DEB-AAPP y DEA-AAPP no cualificados.

6.6.2.7 Políticas de divulgación integradas en la provisión

6.6.2.7.1 Introducción

Durante la emisión del certificado, el Proveedor de Certificados puede crear opcionalmente una política de divulgación integrada para el certificado y proporcionarla a las Unidades de Cartera durante la emisión del certificado. Dicha política de divulgación integrada contiene normas que determinan a qué (tipos de) Parte usuaria (informada) permite el Prestador de certificados recibir la declaración.

Obsérvese que el [Reglamento Europeo de Identidad Digital] no contiene un requisito para que los DIP puedan contener una política de divulgación incorporada, sino sólo para las DECA y las DEA-AAPP.

Para más información sobre las políticas de divulgación incorporadas, consulte el Documento de sobre el Tema D.debate

6.6.2.7.2Tipos de políticas de divulgación incorporadas

El anexo III del [CIR 2024/2979] define las siguientes políticas comunes de divulgación incorporada que deben ser compatibles:

> 1. "Sin política" indica que no se aplica ninguna política a las declaraciones electrónicas de atributos.
> 2. Política de "partes de confianza autorizadas únicamente", que indica que los usuarios de carteras sólo pueden divulgar declaraciones electrónicas de atributos a partes de confianza autenticadas figuren explícitamente en las políticas de divulgación.
> 3. Raíz de específica": indica que los usuarios de monederos sólo deben revelar la Declaración Electrónica de Atributos a las partes usuarias de monederos autenticadas con certificados de acceso de partes usuarias de monederos derivados de una raíz específica (o lista de raíces específicas) o certificado(s) intermedio(s).

La primera de estas políticas es la predeterminada y se aplicará si el Prestador de servicios de certificación no proporciona una política de divulgación integrada para una declaración.

Para expresar las condiciones de las Partes usuarias, una política de divulgación incorporada se referirá a la información incluida en el certificado de registro de la Parte usuaria o en el certificado de acceso proporcionado a la Unidad de Cartera por la Parte usuaria. Tenga en cuenta que los certificados de registro de la Parte usuaria y los certificados de acceso están firmados y, por tanto, la información que contienen está autenticada.

Las Unidades Cartera, así como los mecanismos utilizados para definir y evaluar las políticas, apoyarán al menos las políticas 2. y 3. anteriores. La Comisión velará por que se elabore una especificación técnica sobre el formato de estas políticas. 6.6.2.7.3Distribución de políticas de divulgación integradas

Un Prestador de Certificados proporcionará una política de divulgación incrustada en los metadatos del Emisor especificados en [OpenID4VCI]. Para ello no será necesario modificar el formato de la declaración.

La Comisión velará por que se cree una especificación técnica para la emisión de políticas de divulgación incrustadas.

Además, las políticas se integrarán directamente en los metadatos, en lugar de estar "vinculadas" mediante una URL y almacenadas por el Prestador de servicios de certificación. Este enfoque no requiere que la Unidad Cartera se comunique con el Proveedor de Certificados para poder obtener y evaluar una política para una declaración solicitada por una Parte usuaria (informada). En su lugar, durante la emisión de una ,

la Unidad Cartera recupera cualquier política de divulgación pertinente de los metadatos y la almacena localmente. Una consecuencia de este enfoque es que un Prestador de servicios de certificación revocará una declaración si debe actualizarse una política de divulgación pertinente incrustada.

6.6.2.8 Emisión de lotes

La emisión por lotes significa que, en lugar de emitir un único DIP o declaración a una Unidad Cartera, un Proveedor de DIP o un Proveedor de Declaraciones emite un lote de ellos. Todos los DIP o declaraciones de un lote tienen el mismo tipo de declaración, valores de atributo y período de validez. Aparte de esto, todas descripciones de esta sección 6.6.2 se aplican independientemente del número de declaraciones emitidas (individuales o en lote).

La emisión de lotes se trata con más detalle en el Documento de debate del Tema B.

6.6.3 Presentación del DIP o declaración a la Parte usuaria (informada)

6.6.3.1 Relaciones de confianza necesarias

Una Parte usuaria puede solicitar a un usuario que presente algunos atributos de un DIP o de una declaración en su Unidad Cartera. La figura 11 muestra que una Parte usuaria utiliza una Instancia de Parte usuaria para interactuar con la Unidad de Cartera del . La relación entre la Parte usuaria y su Instancia de Parte usuaria es similar a la relación entre el Usuario y su Unidad Cartera.

Al procesar la solicitud, se establecen las siguientes relaciones de confianza:

1. La Unidad Cartera autentica la Instancia de la Parte de Confianza, asegurando al Usuario sobre la identidad de la Parte de Confianza. En la sección 6.6.3.2 se explica cómo .
2. La Unidad Cartera verifica que la Parte usuaria no solicita más atributos de los que tiene , e informa al usuario del resultado de esta verificación. Para más información, véase la sección 6.6.3.3.
3. El Prestador de Certificaciones, durante la emisión, puede haber incluido opcionalmente una política de divulgación en la declaración. Si dicha política está presente en el certificado solicitado, la Unidad Cartera evalúa la política de divulgación e informa al usuario del resultado de esta evaluación. Véase el apartado 6.6.3.4.

4. El Usuario aprueba o rechaza la presentación de los atributos solicitados. La aprobación del usuario y la presentación selectiva se describen en la sección 6.6.3.5. Posteriormente, después de que la Unidad Cartera presente los atributos seleccionados del DIP o declaración a la Parte usuaria (informada)

   Instancia enviando una respuesta a la solicitud, la Parte usuaria (informada) valida la respuesta. Se establecen las siguientes relaciones de confianza:

5. La Instancia de la Parte usuaria (informada) verifica la firma del DIP o declaración. Esto garantiza que la Parte usuaria puede confiar en que el DIP o la declaración que recibe ha sido emitido por un Prestador auténtico y no ha sido modificado. Esto se describe en la sección 6.6.3.6.
6. La Parte usuaria (informada) verifica que el Proveedor del DIP o el Proveedor del certificado no ha revocado el DIP o la declaración. Esto se describe en la sección 6.6.3.7.
7. La Parte usuaria verifica que el Proveedor de DIP o el Proveedor de atestados emitió este DIP o atestado a la misma Unidad Cartera que lo presentó a la Parte usuaria. En otras palabras, comprueba que el DIP o la declaración no han sido copiados o reproducidos. Esto se denomina generalmente vinculación de dispositivo, y se trata en la Sección 6.6.3.8.
8. En algunos casos de uso, la Parte usuaria verifica que la persona que presenta el DIP o la declaración es el sujeto del DIP o de la declaración. Esto se denomina vinculación del usuario. En otros casos, la Parte usuaria confía en que la Unidad de Cartera y el WSCD lo han hecho. La vinculación del usuario se trata en la Sección 6.6.3.9.
9. La Parte usuaria (informada) puede solicitar atributos de dos o más declaraciones en la misma interacción. Esto se denomina **presentación combinada de atributos**. En tal caso, la Parte usuaria (informada) verifica que estas declaraciones pertenecen al mismo usuario. Esto se trata en la sección 6.6.3.10.

Antes o después de validar el DIP o la declaración según los pasos 5 a 9,

1. La Instancia de la Parte usuaria (informada) autentica la Unidad de Cartera y el Prestador de Cartera; ver Sección 6.6.3.11.
2. La Instancia de la Parte usuaria (informada) verifica que el Proveedor de Carteras no ha revocado la Unidad de Cartera, véase la Sección 6.6.3.12.

Por último, una vez finalizada la interacción con la Instancia de la Parte usuaria (informada),

1. La Unidad de Cartera permite al Usuario denunciar solicitudes ilegales o sospechosas de datos personales por una Parte usuaria (informada), basándose en la información registrada por la Unidad de Cartera. Del mismo modo, la Unidad Cartera permite al Usuario solicitar a una Parte usuaria que elimine datos personales (es decir, atributos de usuario) obtenidos de la Unidad Cartera. Esto se trata en la Sección 6.6.3.13.

6.6.3.2 La Unidad Cartera autentica la Instancia Parte usuaria (informada)

La autenticación de la Parte usuaria es un proceso mediante el cual una Parte usuaria demuestra su identidad a una Unidad de Cartera, en el contexto de una interacción en la que la Parte usuaria solicita a la Unidad de Cartera que

presentar algunos atributos. La autenticación de la Parte usuaria (informada) se trata en el Tema 6.

La autenticación de la Parte usuaria (informada) se incluye en el protocolo utilizado por una Unidad Cartera y una Instancia de Parte usuaria (informada) para comunicarse. Como se documenta en el Tema 12, se pueden utilizar al menos dos protocolos diferentes dentro del ecosistema Cartera IDUE, a saber, los especificados en [ISO/IEC 18013-5] y [OpenID4VP]. Ambos protocolos incluyen funcionalidades que permiten a la Unidad Cartera autenticar la Instancia Parte usuaria (informada). Aunque estos protocolos difieren en los detalles, a un alto nivel, ambos implementan la autenticación de la Parte usuaria (informada) como se muestra en la Figura 12 a continuación.

Figura 12](media/Figure_12_Relying_Party_Authentication.png Figura 12

Resumen de alto nivel del proceso de autenticación de la Parte usuaria (informada)

La figura muestra lo siguiente:

En primer lugar, hay dos condiciones previas que deben cumplirse antes de que pueda comenzar el proceso de autenticación de la Parte usuaria (informada). Nótese que estas acciones no se llevan a cabo para cada presentación, sino una sola vez (excluyendo posibles actualizaciones):

A) La Parte usuaria (informada) se registró como se describe en la Sección 6.4.2 y obtuvo un certificado de acceso a la Instancia de la Parte usuaria (informada).

B) La Unidad Cartera obtuvo el ancla de confianza de la Autoridad de Certificación de Acceso a Instancia de la Parte usuaria (informada).

Posteriormente, durante cada presentación de atributos:

1. La Instancia de la Parte usuaria prepara una solicitud de algunos atributos a la Unidad Cartera e incluye su certificado de acceso a la Instancia de la Parte usuaria en la solicitud, además de todos los certificados intermedios hasta (pero excluyendo) el ancla de confianza.
2. La Instancia de la Parte usuaria (informada) firma algunos datos de la solicitud de atributos utilizando su clave privada.
3. La Instancia Parte usuaria (informada) envía la solicitud a la Unidad Cartera.
4. La Unidad Cartera comprueba la autenticidad de la solicitud verificando la firma sobre la solicitud utilizando la clave pública del certificado de acceso a la Instancia de la Parte usuaria (informada).
5. La Unidad Cartera comprueba la autenticidad de la Parte usuaria (informada) validando el certificado de acceso a la Instancia de la Parte usuaria y todos los certificados intermedios incluidos en la solicitud. Para validar el último certificado intermedio, la Unidad Cartera utiliza el ancla de confianza que obtuvo de la Lista de Confianza.

6. La Unidad Cartera valida que ninguno de los certificados de la cadena de confianza ha sido revocado. Esto incluye el certificado de acceso a la Instancia de la Parte usuaria, así como todos los demás certificados de la cadena de confianza, incluido el propio anclaje de confianza, si procede.
7. La Unidad Cartera continúa solicitando la aprobación del Usuario.
8. El usuario aprueba los atributos que se presentarán.
9. La Unidad Cartera envía una respuesta que contiene sólo los atributos aprobados a la Instancia Parte usuaria (informada).

6.6.3.3 Unidad Cartera permite a la Parte usuaria verificar que no solicita más at- tributos de los que tiene registrados

Durante la inscripción, la Parte usuaria (informada) registra qué atributos pretende solicitar a las Unidades Cartera. El Registrador enumera estos atributos en un certificado de registro de Parte usuaria y lo envía a la Parte usuaria, que lo distribuye a todas sus Instancias de Parte usuaria.

Durante una transacción, una Instancia de Parte usuaria envía este certificado de registro a la Unidad de Cartera en la solicitud de presentación. La Unidad Cartera muestra el contenido del certificado de registro al Usuario cuando le pide su aprobación, véase el apartado 6.6.3.5, al menos en caso de que uno o varios de los atributos solicitados no estén incluidos en la lista de atributos del certificado de registro.

El formato del certificado de registro, así como la forma en que la Unidad Cartera puede verificar que el certificado de registro pertenece a la Parte usuaria (informada) autenticada, se especificarán en una especificación técnica. Para más información, véase el Tema 44.

6.6.3.4 La Unidad Cartera evalúa la política de divulgación incorporada, si existe

Durante la emisión de la declaración, el Prestador de servicios de certificación puede crear una política de confidencialidad incrustada para la declaración (véase la sección 6.6.2.7). Si dicha política está presente para la atestación solicitada, la Unidad Cartera evalúa la política, junto con la información del certificado de acceso o del certificado de registro presentado por la Parte usuaria, para determinar si el Prestador de atestados permite a esta Parte usuaria recibir la atestación solicitada. Tenga en cuenta que la Unidad Cartera verifica la autenticidad de estos certificados antes de utilizar cualquier dato contenido en ellos.

La Unidad Cartera presenta el resultado de la evaluación de la política de divulgación al Usuario en forma de aviso, cuando solicita la aprobación del Usuario. Por ejemplo, "El emisor de sus datos médicos no desea que presente datos de <nombre de la declaración> a <nombre de la Parte usuaria (informada)>. ¿Desea continuar?". Tenga en cuenta que el Usuario puede anular el resultado de la evaluación de la política de divulgación.

Para más detalles sobre la política de divulgación de información implícita, véase el Tema 43.

6.6.3.5 La Unidad Cartera obtiene la aprobación del Usuario para presentar los atributos seleccionados

Nota: En este documento, el término aprobación del usuario" se refiere exclusivamente a la decisión de un de presentar un atributo a una Parte usuaria (informada). En ningún caso la aprobación del Usuario

para presentar datos de su Unidad Cartera debe interpretarse como fundamento legal para el tratamiento datos personales por la Parte usuaria (informada) o cualquier otra entidad. La Parte usuaria (informada) que solicite o procese datos personales de una Unidad Cartera debe asegurarse de que tiene motivos para procesar legalmente esos datos, de conformidad con el artículo 6 del RGPD.

Antes de presentar cualquier atributo a una Parte usuaria (informada), la Unidad Cartera solicita al Usuario su aprobación. Esto es fundamental para garantizar que el usuario mantiene el control de sus atributos.

Una Unidad Cartera solicita la aprobación del Usuario en todos los casos de uso, tanto en el flujo de proximidad como en el flujo remoto, e incluyendo:

- Casos de uso en los que se puede suponer que la Parte usuaria (informada) es de confianza, por ejemplo, cuando la Parte usuaria (informada) forma parte de las fuerzas de seguridad u otro organismo gubernamental.
- Casos de uso en los que los atributos solicitados son fundamentales para que la Parte usuaria (informada) conceda acceso al usuario o preste los servicios solicitados.
- Casos de uso en los que no existe, de acuerdo con el GDPR u otra legislación, ninguna necesidad legal de solicitar la aprobación del Usuario porque existe otra base legal para solicitar los atributos.

Un requisito previo para solicitar la aprobación del Usuario es que la Unidad Cartera esté segura de que la persona que utiliza la Unidad Cartera es de hecho el Usuario. Por lo tanto, la WSCA autentica al Usuario antes o durante la solicitud de aprobación del Usuario, a petición de Cartera. Para ello, la Unidad Cartera utiliza los mecanismos de autenticación del Usuario establecidos durante la activación de la Unidad Cartera, véase la Sección 6.5.3. Se pueden encontrar requisitos más detallados relativos a la aprobación del Usuario en el Tema 6.

Otro prerrequisito para la aprobación efectiva del Usuario es que la Unidad Cartera permita la divulgación selectiva de atributos. La divulgación selectiva implica principalmente dos cosas. En primer lugar, permite a una Parte usuaria (informada) especificar qué atributos de una declaración desea recibir (y cuáles no). Una Parte usuaria (informada) puede tener diferentes propósitos para los solicitados. Por ejemplo, una tienda de licores en línea puede necesitar una declaración de edad para cumplir sus obligaciones legales y, además, desearía recibir información sobre la dirección para poder enviar el licor solicitado al domicilio del usuario. Por lo tanto, la Parte usuaria (informada) indica el objetivo de cada (grupo de) atributos solicitados.

En segundo lugar, la divulgación selectiva implica que la Unidad Cartera permite al Usuario aprobar o denegar la presentación de cada (grupo de) atributos por separado. El Usuario toma una decisión al menos en la siguiente información:

- Identidad autenticada de la Parte usuaria (informada),
- La información del certificado de registro de la Parte usuaria (informada) relativa a los atributos que ésta ha registrado durante el registro, al menos en caso de que uno o varios de los atributos solicitados no figuren en la lista de atributos del certificado de registro,
- La información que figura en el certificado de registro de la Parte usuaria (informada) relativa a un intermediario utilizado por la Parte usuaria (informada), en su caso; véase la sección 3.11.
- El resultado de la evaluación de la política de divulgación incorporada, en caso.

Después de que el Usuario dé su aprobación, la Unidad Cartera presentará los atributos de Usuario aprobados a la Instancia Parte usuaria (informada).

6.6.3.6 Parte usuaria (informada) verifica la autenticidad del DIP o de la declaración

La Instancia de la Parte usuaria (informada) recibe un DIP o declaración, incluyendo algunos atributos, de la Unidad Cartera. Posteriormente, verifica la firma sobre el DIP o declaración. Para ello, en el caso de los DIP y las DECA, la Instancia de la Parte usuaria utiliza un ancla de confianza del Prestador obtenida de una Lista de confianza. Obsérvese que el Prestador de DIP o el Prestador de DECA puede utilizar un certificado de firma intermedio para firmar el DIP o la declaración, y utilizar el anclaje de confianza para firmar el certificado de firma, en lugar de firmar el DIP o la declaración directamente con el anclaje de confianza.

En el caso de los DEA-AAPP, la Instancia de la Parte usuaria verifica un DEA-AAPP comprobando en primer lugar la firma del Prestador del DEA-AAPP sobre el DEA-AAPP, utilizando el certificado del Prestador del DEA-AAPP emitido por un QTSP. Posteriormente, la Instancia de la Parte usuaria (informada) verifica la firma sobre este , utilizando el anclaje de confianza correspondiente de la Lista de confianza de QTSP. Nótese que tanto el Prestador DEA-AAPP como el QTSP pueden utilizar un certificado de firma intermedio. En igualdad de condiciones, la verificación de una DEA-AAPP implicará, por tanto, uno o más certificados adicionales, en comparación con la verificación de una DIP o una DECA.

Por último, en el caso de las DEA no cualificadas, las Directrices de elaboración aplicables podrán describir el modo en que la Instancia de la Parte usuaria obtiene el anclaje de confianza pertinente.

Lo anterior implica que una Instancia de Parte usuaria es consciente de si la declaración que solicita a una Instancia de Cartera es un DIP, una DEA, una DEA-AAPP o una DEA no cualificada. Además, la Instancia de la Parte usuaria almacena anclas de confianza de tal forma que, en el momento de la verificación, es capaz de distinguir entre anclas de confianza utilizables para DIP, para QEAA, para DEA-AAPP o para CEA no cualificadas.

La implementación técnica del proceso de verificación de firma depende de cuál de los estándares mencionados en el Tema 12 es soportado por la Unidad Cartera. Cada uno de estos especifica en detalle cómo llevar a cabo la verificación de firma.

Además, es posible que la Parte usuaria (informada) desee comprobar que el Proveedor de certificados puede expedir legalmente el tipo de declaración en . Como se describe en la sección 6.3.2.2, esto sólo es necesario para los proveedores de CEA no cualificados, ya que la Parte usuaria confía en un proveedor de DIP, un proveedor de DEA o un proveedor de DEA-AAPP. En el caso de los Proveedores de DEA, las Directrices de elaboración aplicables pueden definir métodos que la Parte usuaria puede utilizar para verificar que el Proveedor de DEA está autorizado a emitir este tipo de declaración.

Notas:

- Todos los DIP y declaraciones del ecosistema de Cartera IDUE están firmados digitalmente por el respectivo Prestador de DIP o Prestador de Declaración, o por un WSCD que forma parte de la Unidad de Cartera. Si una declaración está firmada digitalmente por un WSCD, se denomina declaración firmada por dispositivo o autoemitida. Los DIP o declaraciones firmados por el dispositivo o

autoemitidos sólo están permitidos si puede demostrarse que el WSCD los firma con el Nivel de Aseguramiento (LoA) requerido. Esto implica que el nivel de seguridad ofrecido por el WSCD es al menos equivalente al nivel de seguridad de la infraestructura segura utilizada por el Prestador de DIP o el Prestador de Certificados para firmar los DIP o las declaraciones.

- La firma sobre el DIP o la declaración puede incluir o no el valor de los atributos enviados previamente. Si los valores de los atributos no se incluyen en la creación de la firma, la Parte usuaria confía en estos atributos porque se presentan a través de un canal autenticado establecido entre el entorno seguro (es decir, el WSCD o la infraestructura segura utilizada por el Prestador del DIP o el Prestador del certificado, véase el punto anterior) y la Parte usuaria. Una forma posible de establecer este canal autenticado es garantizar la autenticidad e integridad (pero no el no repudio) de los atributos mediante un Código de Autenticación de Mensaje MAC). El MAC es creado por el entorno seguro sobre los valores de atributos presentados. La clave MAC se genera a partir de una clave efímera de la Parte usuaria (enviada al entorno seguro por la Instancia Cartera) en combinación con una clave efímera creada por el entorno seguro. Esta última clave efímera se envía a la Parte usuaria (informada) de forma que ésta pueda verificar la autenticidad de dicha clave. Esta solución, u otras similares, pueden utilizarse siempre que:

  - la solución cumple plenamente las normas pertinentes, es decir, [ISO/IEC 18013-5] u [OpenID4VP] y [SD-JWT VC].
  - la solución puede certificarse para la seguridad en LoA "alto" según el capítulo 7

6.6.3.7 Parte usuaria (informada) verifica que el DIP o la declaración no han sido revocados

Para permitir la comprobación de la revocación de un DIP o una declaración, el Prestador de DIP o el Prestador de Declaraciones incluye información sobre la revocación en el DIP o la declaración, si su validez es superior a 24 horas. Esta información de revocación incluye una URL que indica la ubicación en la que una Parte usuaria (informada) puede obtener una lista de estado o una lista de revocación, y un identificador o índice para este certificado o atestación específico dentro de esa lista.

Notas:

- En el caso de las declaraciones con un período de validez inferior a 24 horas, no es necesario incluir información sobre la revocación.
- Una lista de estado es una cadena de bits o de bytes en la que cada bit o grupo de bits denota el estado de revocación actual (válido o revocado) de una declaración. Para conocer el estado de la declaración que ha recibido de la Unidad Cartera, la Parte usuaria (informada) obtiene la lista de estado de la URL especificada en la declaración y verifica el valor codificado en la posición de bit dada por el valor de índice en la declaración.
- Una lista de revocación es una lista de identificadores de DIP o de declaraciones revocados por el Prestador de DIP o el Prestador de Declaraciones. Para conocer el estado del DIP o de la declaración que ha recibido de la Unidad Cartera, la Parte usuaria (informada) obtiene la lista de revocación de la URL especificada en la declaración y comprueba si el identificador incluido en la declaración figura o no en la lista.

Para más detalles y requisitos sobre la revocación, véase el Tema 7.

6.6.3.8 Parte usuaria (informada) verifica la vinculación del dispositivo

La vinculación a dispositivos es la propiedad por la que un DIP o una declaración están vinculados a un dispositivo específico (de hecho, un WSCD) y no pueden utilizarse independientemente de dicho dispositivo. La vinculación a dispositivos protege la declaración frente a copias o clonaciones, lo que aumenta su seguridad.

Un Prestador de DIP o un Proveedor de atestación implementa la vinculación de dispositivos incluyendo una clave pública criptográfica en el DIP o la atestación y . La clave privada correspondiente está protegida por un WSCD certificado en la Unidad Cartera.

El Tema 9 explica que un WSCD genera un par de claves pública-privada para cada declaración a petición de Unidad Cartera, y que la Unidad Cartera envía la clave pública al Proveedor de DIP o al Proveedor de Certificados. Además, discute cómo el DIP o el Proveedor de atestaciones puede verificar que la clave privada correspondiente está realmente protegida por el WSCD.

Durante una interacción, la Parte usuaria (informada) verifica que el DIP o declaración que ha recibido de una Unidad Cartera está efectivamente vinculado al WSCD incluido en la Unidad Cartera. Para ello, la Parte usuaria (informada) solicita a la Unidad Cartera que firme algunos datos utilizando la clave privada correspondiente a la clave pública del DIP o declaración. Por este motivo, la vinculación del dispositivo también se denomina "prueba de posesión". En [ISO/IEC 18013-5] se denomina 'autenticación mdoc'. En [SD-JWT VC] se denomina "vinculación de claves".

La implementación técnica de esta verificación depende de cuál de las normas mencionadas en el Tema 12 soporta la Unidad Cartera. Cada uno de estos estándares especifica en detalle cómo llevar a cabo esta verificación.

6.6.3.9 Instancia Parte usuaria (informada) verifica o confía en la vinculación del usuario

La vinculación del usuario (a veces también denominada "vinculación del titular") es la propiedad de que el sujeto del DIP o de la declaración, es decir, la persona física o jurídica descrita en él, es de hecho la persona que presenta el DIP o la declaración a la Parte usuaria (informada). La vinculación del usuario impide que un atacante presente con éxito un DIP o una declaración que no está legalmente autorizado a utilizar.

El mecanismo o mecanismos disponibles para la vinculación del usuario dependen del tipo de flujo de presentación (de proximidad o remoto, supervisado o no supervisado, véase también la sección 4.4), y de los atributos emitidos al usuario por el Prestador de DIP o el Prestador de declaraciones:

1. En primer lugar, la Parte usuaria (informada) siempre puede decidir confiar en los mecanismos de autenticación de usuario implementados por el WSCD (véase el Tema 9). Esto significa que la Parte usuaria confía en que el WSCD ha autenticado correctamente al usuario antes de presentar los atributos. Tenga en cuenta que:

- Esta confianza no se basa en el resultado de ninguna verificación por parte de la Parte usuaria, sino en una confianza a priori en (en particular) el WSCD certificado que forma parte de la Unidad Cartera.
- El uso de este método implica que las Partes usuarias también confían en la vinculación del dispositivo, tal y como se describe en la Sección 6.6.3.8. De hecho, la Instancia de la Parte usuaria verifica en primer lugar que el DIP o la declaración están vinculados a un WSCD en el que confía el Prestador del DIP o el Prestador de la declaración y, a continuación, confía en que el WSCD ha autenticado correctamente al usuario.
- De hecho, este método de vinculación del Usuario siempre se llevará cabo, ya que el WSCD debe autenticar a su Usuario cuando solicita la aprobación del Usuario para presentar cualquier atributo, y ya que la vinculación del dispositivo también es obligatoria.

2. Además, en algunos casos, si una Parte usuaria no desea confiar únicamente en el mecanismo anterior, podrá utilizar atributos de usuario para llevar a cabo una vinculación de usuario adicional proceso. Por ejemplo, si el DIP o la declaración contienen un retrato del usuario, la Parte usuaria (informada) podrá comparar visual o biométricamente dicho retrato con la cara de la persona que presenta la declaración o mediante una foto tomada por una máquina automatizada o como "selfie". Por lo general, esto será posible en presentaciones de proximidad supervisadas por inspección humana, o en un flujo de proximidad no supervisado si se dispone del equipo adecuado. También puede ser posible hacerlo en presentaciones a distancia no supervisadas mediante el uso de tecnología de reconocimiento facial, posiblemente incluso a distancia. Sin embargo, para generar resultados fiables en tales situaciones, se requieren condiciones especiales y medidas de seguridad específicas, como una buena iluminación, instrucciones claras para que el usuario coloque su cara y un mecanismo aprobado de detección de vitalidad que apoye la detección de ataques de presentación (PAD), así como mecanismos para la detección de ataques de inyección, en particular la detección de deepfake.
3. Por último, si la persona que presenta el DIP o la declaración puede presentar un documento de identidad, la Parte usuaria (informada) podrá verificar la vinculación del usuario comparando los atributos del DIP o de la declaración, como el nombre y los , con los del documento de identidad. Sin embargo, esto requiere que la Parte usuaria (informada) pueda verificar que el documento de identidad es auténtico y pertenece realmente a la persona que lo presenta. En la práctica, esto significará a menudo que el documento de identidad es un documento de identidad con fotografía, por lo que la presentación deberá hacerse en proximidad y ser supervisada, o hacerse a distancia y con el apoyo de un PAD.

Por último, nótese que en una presentación combinada de atributos según la sección siguiente, si se demuestra la vinculación del usuario para una de las presentadas, se demuestra para todas ellas.

6.6.3.10 Instancia Parte usuaria (informada) verifica la presentación combinada de atributos

Según el [Reglamento Europeo de Identidad Digital], una presentación combinada de atributos es una solicitud de atributos de dos o más declaraciones en la misma acción. En este caso, la Parte usuaria

(informada) verificará que estas declaraciones pertenecen al mismo usuario, para evitar que una Unidad de Cartera pirateada o fraudulenta presente atributos de diferentes usuarios.

La Parte usuaria (informada) puede comprobarlo comparando los atributos de las distintas declaraciones. Por ejemplo, la Parte usuaria () puede solicitar el nombre y los apellidos del usuario en todas las certificaciones y comparar los nombres. Si coinciden, la Parte usuaria (informada) concluye que las declaraciones pertenecen al mismo usuario. Sin embargo, este método implica que la Parte usuaria (informada) debe solicitar información de identificación al usuario. En algunos casos de uso, solicitar esa información puede no ser estrictamente necesario, por lo que este método puede considerarse una amenaza para la privacidad del usuario. Además, este método puede no ser concluyente, por ejemplo si varias personas comparten el mismo nombre.

Para resolver estos inconvenientes, el Tema 18 describe cómo la Instancia de la Parte usuaria (informada) puede verificar esto criptográficamente comprobando que las claves privadas emparejadas con las claves públicas en las atestaciones están protegidas por el mismo WSCD. Esto se describe con más detalle en el Tema 9.

6.6.3.11 La Instancia de la Parte usuaria autentica la Unidad de Cartera y el Prestador de Cartera.

La sección 6.5.3 anterior describe que un Prestador de Cartera, durante la vida de una Unidad de Cartera, se asegura de que la Unidad de Cartera esté siempre en posesión de una o más Declaraciones de Unidad de Cartera (WUAs) válidas. Antes o después de solicitar uno o más DIP o declaraciones de una Unidad Cartera, una Instancia Parte usuaria (informada) puede:

- solicitar una WUA a la Unidad Cartera.
- verificar la firma sobre la WUA utilizando el ancla de confianza del Prestador de Cartera obtenida de la Lista de Confianza del Prestador de Cartera.
- verificar que la Unidad Cartera está en posesión de la clave privada perteneciente a la clave pública de la WUA. Esto demuestra que la Unidad Cartera es auténtica y que la proporciona el Prestador de Carteras de confianza.

Tenga en cuenta que solicitar y verificar la WUA no es obligatorio.

6.6.3.12 Parte usuaria (informada) verifica que la WUA no está revocada

En la sección 6.6.2.4 se explica cómo un Prestador de DIP o un Prestador de Declaraciones puede verificar que una UAE (y, por tanto, la Unidad Cartera) no ha sido revocada. Las Instancias de Parte usuaria (informada) también pueden utilizar el mismo mecanismo.

6.6.3.13 La Unidad Cartera permite al usuario informar de solicitudes sospechosas de una Parte usuaria (informada) y solicitar a una Parte usuaria (informada) que borre datos personales.

Una Unidad Cartera permite al Usuario informar a una Autoridad de Protección de Datos APD) sobre solicitudes ilegales o sospechosas de datos personales por parte de una Parte usuaria (informada). Para , una Unidad Cartera proporciona un tablero de mandos que permite al Usuario presentar una denuncia sobre una solicitud de presentación sospechosa de la Parte que Confía ante la APD del Estado miembro que proporcionó su Unidad Cartera. Para más información y requisitos, véase el Tema 50. El Usuario puede realizar dicha denuncia independientemente de si realmente se presentó algún atributo a la Parte usuaria (informada). Incluso si la Instancia de Cartera impidió la presentación de cualquier atributo porque falló la autenticación de la Parte usuaria, o si el Usuario

no aprobó la presentación de ningún atributo, el Usuario aún puede presentar una reclamación sobre la solicitud ante la Autoridad de Protección de Datos pertinente.

El panel de control también permite al usuario solicitar a una Parte usuaria (informada) que borre sus datos personales. Para más información y requisitos, véase el Tema 48.

Para poder fundamentar una reclamación, o enumerar los datos que deben eliminarse, el usuario necesita estar informado sobre qué atributos fueron solicitados por qué Parte usuaria (informada). Para ello, una Unidad Cartera mantiene un registro de todos los atributos solicitados y presentados. El panel de control mencionado anteriormente también permite al usuario ver el registro y presentar una reclamación sobre cualquier atributo del registro. Encontrará más información sobre la función de registro en el Tema 19.

6.6.4 Presentación del DIP o declaración a otra Unidad Cartera

En la Sección 6.6.3 se trataron las relaciones de confianza necesarias cuando una Unidad Cartera recibe una petición de una Instancia Parte usuaria y presenta atributos a esa Instancia Parte usuaria (informada).

Sin embargo, el [Reglamento Europeo de Identidad Digital] exige que una Unidad de Cartera también pueda recibir una solicitud de este tipo de otra Unidad de Cartera y presentar atributos a la Unidad de Cartera solicitante. Para más información y requisitos, consulte el Tema 30.

6.6.5 Gestión de DIP o declaraciones

6.6.5.1 Visión general

A partir de la emisión de un DIP o declaración, el DIP o declaración es gestionado por el Usuario y el Prestador de Carteras. La gestión se lleva a cabo hasta que el DIP, o declaración, es eliminado o la Instancia Cartera es desinstalada por el Usuario. La gestión incluye al menos los siguientes procesos:

1. Reexpedición del DIP o declaración cuando sea necesario.
2. Revocación del DIP o de la declaración cuando sea necesario.

Estos procesos se tratan en las siguientes subsecciones.

6.6.5.2 Reexpedición del DIP o de la declaración

6.6.5.2.1 Introducción

Por reemisión se entiende la sustitución de un DIP o certificado ya existente en una Unidad Cartera por un DIP o certificado del mismo tipo. La reemisión la realiza siempre el mismo Prestador de DIP o Prestador de atestados que emitió el DIP o atestado existente y la inicia la Unidad Cartera. El valor de los atributos en la nueva declaración será normalmente el mismo que en la declaración original. Sin embargo, esto no es obligatorio; el Prestador de DIP o el Prestador de atestados pueden cambiar uno o más valores de atributos. La reexpedición sólo se aplica dentro del periodo de validez administrativa de un documento. Por ejemplo, un Carné de Conducir Móvil (mDL) suele expedirse en forma de declaraciones que tienen un periodo de validez técnica inferior al periodo de validez administrativa del propio carné. La reemisión se utiliza para obtener nuevas declaraciones según sea necesario durante el de validez administrativa, para garantizar que el usuario siempre pueda compartir un carné de conducir móvil válido. Sin embargo, cuando finalice el periodo de validez administrativa, habrá un proceso para obtener un nuevo permiso de conducción administrativo, que sin embargo queda fuera del ámbito de este documento.

Tenga en cuenta que, en general, si el DIP o la declaración originales se expidieron en un lote, el Prestador de DIP o el Prestador de Declaraciones volverá a expedir ese DIP o esa declaración en un lote.

Puede haber diferentes motivos para volver a expedir un DIP o una declaración, por ejemplo:

- Los DIP o declaraciones actuales están a punto de finalizar su período de validez técnica, o la Unidad Cartera se está quedando sin declaraciones únicas. Esto se hace para mitigar el riesgo de vinculabilidad de la Parte usuaria (informada). Para más información, véase la sección 7.4.3.5.
- Ha cambiado el valor de uno o varios de los atributos del DIP o de la declaración.
- La arquitectura de seguridad de la Solución Cartera puede utilizar DIP y/o declaraciones que se emiten justo en el momento en que la Parte usuaria (informada) solicita el DIP o la declaración. Esto se denomina a veces emisión sincrónica.

Estas razones se analizan en las siguientes subsecciones. La reemisión se trata con más detalle en el Documento de debate del Tema B.

6.6.5.2.2 Reemisión para limitar la vinculabilidad de la Parte usuaria (informada)

Tal como se especifica en [ISO/IEC 18013-5] o [SD-JWT VC], cada DIP o declaración contiene metadatos que indican su período de validez técnica. La determinación de la duración del período de validez técnica es responsabilidad del Prestador del DIP o del Proveedor de la declaración. El período de validez técnica elegido el Prestador de DIP o el Proveedor de Certificados dependerá de varios factores, principalmente la arquitectura de seguridad de la Solución Cartera y la estrategia elegida para mitigar la vinculabilidad de la Parte usuaria (informada), véase el apartado 7.4.3.5.

Teniendo en cuenta los factores anteriores, en general puede asumirse que el periodo de validez técnica de un DIP o de una declaración será mucho más corto que su vida útil, es decir, el periodo de tiempo que un Usuario desea mantener ese DIP o esa declaración en su Unidad Cartera. Esto implica que será necesario

emitir nuevos DIP y declaraciones periódicamente, para sustituir a los que estén llegando al final de su validez técnica.

Una razón similar para volver a emitir DIP y declaraciones se da cuando el Prestador de DIP o el Prestador de Declaraciones utiliza declaraciones de una sola vez (véase el apartado 7.4.3.5), que sólo pueden presentarse una vez a una Parte usuaria (informada). En ese caso, la Unidad Cartera, o más bien el Usuario, necesitará periódicamente nuevos DIP o declaraciones para no quedarse sin ellos.

La reexpedición de DIP o declaraciones por estos motivos es una cuestión puramente técnica. En la medida de lo , el usuario no se da cuenta de que se ha vuelto a expedir un DIP o una declaración, ni tiene que tomar ninguna medida para garantizar que la reexpedición se produzca a tiempo. Estas condiciones son muy diferentes de las de la primera expedición de un DIP o una declaración, en las que el usuario debe tomar la iniciativa de solicitar el DIP o la declaración, y también puede participar en el proceso de otras maneras.

Esto implica, entre otras cosas, que no puede producirse ninguna autenticación del Usuario durante la reemisión de una declaración existente. No obstante, una Unidad Cartera puede ofrecer al Usuario la opción de recibir una notificación de reemisión.

En ausencia de autenticación de usuario, y para evitar que un DIP o una declaración reemitidos acaben en el usuario equivocado, el Proveedor de DIP o el Proveedor de declaraciones garantiza que el DIP o la declaración reemitidos están vinculados al mismo WSCD que el DIP o la declaración a los que sustituyen.

Por último, dado que el usuario no interviene, es la Unidad Cartera la que activa la reemisión de DIP y la declaración cuando es necesario.

6.6.5.2.3 Reemisión por cambio de valores de atributos

Durante la vida de un DIP o de una declaración, el valor de algunos de los atributos puede cambiar. Por ejemplo, en la fecha de nacimiento del Usuario, un atributo de declaración de edad (es decir, un atributo que indica si el Usuario ha alcanzado una determinada edad) puede tener que cambiar de valor Falso a valor Verdadero. En otro ejemplo, el Usuario de un permiso de conducción móvil puede haber aprobado el examen para una categoría de vehículo diferente. En este caso, el Prestador de DIP o el Prestador de atestados volverá a expedir el DIP o el atestado con los valores de atributo correctos, y revocará el atestado existente.

La reemisión de un DIP o una declaración por este motivo repercutirá en el usuario, ya que se dará cuenta de que se han modificado los valores de sus atributos. Por lo tanto, en este caso se informará a los usuarios cuando se produzca la reemisión. Además, un Prestador de servicios de certificación puede declarar en sus condiciones que puede recurrirse a la reemisión de un certificado.

6.6.5.2.4 Reemisión cuando se utiliza la emisión síncrona

Una tercera razón para volver a emitir un DIP o una declaración es cuando el Prestador de DIP o el Prestador de Declaraciones utiliza la emisión sincrónica en su arquitectura de seguridad. En una arquitectura de este tipo, la Unidad Cartera solicita la emisión de un nuevo DIP o atestación después de haber recibido una solicitud de ese DIP o atestación de una Parte usuaria (informada). Estos DIP o declaraciones duran muy poco y sólo se utilizan una vez.

En el ámbito de este documento, este motivo de reexpedición es muy similar a los motivos expuestos en el apartado 6.6.5.2.

6.6.5.3DIP o revocación de la declaración

La gestión de DIP o declaraciones incluye garantizar que los DIP y las declaraciones puedan revocarse en caso necesario. La revocación se trata en el Tema 7. El Usuario puede solicitar al Proveedor de DIP o al Proveedor de Certificados que revoque el DIP o la declaración al menos en caso de pérdida o robo. Además, un Proveedor de DIP o un Proveedor de atestados podría verificar regularmente, para cada uno de sus DIP o atestados válidos, si el Proveedor de Carteras revocó la Unidad de Cartera en la que reside ese DIP o atestado. Si resulta que la Unidad de Cartera está , el Proveedor de DIP o el Proveedor de Atestados podría revocar el DIP o atestado respectivo. Por el momento, no se ha especificado ningún mecanismo que permita a un Prestador de DIP o a un Proveedor de Certificados verificar si una Unidad de Cartera ha sido revocada. Esto se debatirá en el ARF 2.0.

6.6.6 Supresión del DIP o de la declaración

En caso de que el Usuario ya no desee conservar un DIP o una declaración específicos en su Unidad Cartera, puede . Si el Prestador de DIP o el Prestador de atestados ha emitido un lote de varios DIP o atestados que tienen el mismo contenido y son válidos, la Unidad Cartera los borra todos. Borrar un DIP o una declaración también significa que el WSCD destruye el material de clave criptográfica asociado a ese DIP o declaración. Antes de eliminar el DIP o la declaración y las claves criptográficas, la WSCA incluida en la Unidad Cartera autenticará al Usuario.

Si admite la API de credenciales digitales, véase la sección 4.4.3, la Unidad Cartera también revela el hecho de que ya no contiene el DIP o la declaración al marco de la API de credenciales digitales.

Para más información sobre este tema, véase el Tema 51.

7 Certificación y gestión de riesgos

7.1 Introducción

En este capítulo se describe brevemente la certificación de las soluciones Cartera y los sistemas de identificación electrónica en los que se basan, así como el enfoque general de certificación, los principios de diseño y los requisitos clave descritos en el Reglamento Europeo de Identidad Digital y el Reglamento de Ejecución de la Comisión (CIR) por el que se establecen normas para la certificación de soluciones Cartera (2024/2981CIR 2024/2981.), o simplemente Además, se hace referencia al Anexo I del CIR, el Registro de Riesgos, que apoya el enfoque basado en el riesgo de las Soluciones Cartera. Para requisitos más detallados, consulte la propia CIR 2024/2981.

El Reglamento Europeo de Identidad Digital exige la certificación de las Soluciones Cartera para garantizar la conformidad de las Soluciones Cartera con los requisitos funcionales, de seguridad y relacionados con la privacidad, a fin de lograr un alto nivel de interoperabilidad, seguridad y fiabilidad. La certificación se aplica

a las Soluciones Cartera y a los esquemas de identificación electrónica bajo los que se proporcionan; para facilitar la lectura, este capítulo sólo se refiere a las Soluciones Cartera. Además, el objeto de la certificación incluye componentes de software, componentes de hardware (en los casos en que sean proporcionados directa o indirectamente por el Prestador de Carteras) y los procesos que soportan la provisión y el funcionamiento de una Solución Cartera, como la activación de la Unidad Cartera, véase la Sección 6.5.3.

El objetivo es armonizar la aplicación de los requisitos establecidos por el [Reglamento Europeo de Identidad Digital] y evitar al máximo los enfoques divergentes. Por esta razón, la Comisión solicitó a ENISA que preparara un sistema de certificación europeo candidato en el marco de la Ley de Ciberseguridad, la CSA. Dado que la definición y adopción de un sistema de certificación específico y armonizado para las soluciones Cartera depende de los acuerdos entre los Estados miembros sobre los requisitos de seguridad detallados, de la disponibilidad de sistemas de certificación subyacentes y de las buenas prácticas establecidas en los propios Estados miembros, se prevé un enfoque transitorio mediante sistemas de certificación nacionales.

En otras palabras, el planteamiento de certificación de las soluciones Cartera sigue dos fases. A corto plazo, los Estados miembros ofrecerán sistemas nacionales (transitorios) de certificación. A medio plazo, se establecerá un sistema CSA armonizado. Cuando el sistema basado en la CSA esté disponible, sustituirá a los sistemas nacionales en lo que respecta a los requisitos de ciberseguridad. Los regímenes podrán seguir existiendo para los requisitos funcionales.

7.2. Certificación de las soluciones Cartera según los sistemas nacionales de certificación

Hasta que se disponga de un sistema de certificación de la ciberseguridad de las soluciones Cartera en el marco de la CSA, el [Reglamento sobre la identidad digital europea] exige a los Estados miembros que establezcan sistemas nacionales de certificación. Esto se hará a tiempo para que las soluciones Cartera estén disponibles antes de finales de 2026. La Comisión ha adoptado el CIR 2024/2981 para establecer los principales requisitos que deben cumplir los Estados miembros para crear regímenes nacionales de certificación. El CIR 2024/2981 y los regímenes nacionales de certificación resultantes se definen en torno a una serie de principios rectores:

En primer lugar, el objetivo es armonizar los requisitos en la medida de lo posible. También se anima a los Estados miembros a colaborar en el diseño y la aplicación de los sistemas nacionales. Además, los regímenes nacionales aprovecharán el uso de los regímenes y normas de certificación pertinentes y existentes para la certificación y evaluación de las soluciones Cartera. Cuando existan, deberán utilizarse los sistemas CSA europeos pertinentes. En la actualidad, sólo está disponible el esquema de certificación de ciberseguridad EUCC basado en los Criterios Comunes para la certificación de ciberseguridad de productos, partes o componentes de productos TIC. Los próximos esquemas basados en CSA incluyen EUCS y EU5G. Además, otros regímenes existentes o futuros son los basados en FITCEM (EN 17640), los nacionales, como los de verificación de identidad a distancia, u otros privados (por ejemplo, para dispositivos móviles y aplicaciones). Para la armonización de los requisitos funcionales, se hace referencia a los Reglamentos de Ejecución de la Comisión adoptados en virtud del artículo 5, letra a), del Reglamento Europeo de Identidad Digital. Para la armonización de los requisitos de certificación, se utiliza el marco ISO/IEC 17065 en virtud del Reglamento [765/2008], complementado por ISO/IEC 17067 sobre la definición de esquemas.

A continuación, el CIR 2024/2981 hace referencia a la naturaleza compuesta de las Soluciones Cartera, así como a las posibles diferentes arquitecturas en los Estados miembros, teniendo en cuenta que el

Reglamento de Identidad Europeo Digital es tecnológicamente (y arquitectónicamente) neutro. Esto significa que la certificación final ("nivel superior") de la solución Cartera dará lugar a un certificado compuesto, basado en la certificación de componentes separados, como la certificación EUCC. Las Soluciones Cartera deben certificarse siempre con un nivel de garantía "alto", tal como se establece en el Reglamento Europeo de Identidad Digitalel CIR (UE) 2015/1502., así como en Ese nivel de garantía debe ser alcanzado por la solución de cartera en su conjunto. En virtud del presente Reglamento, algunos componentes de la solución Cartera podrán certificarse con un nivel de garantía inferior, siempre que esté debidamente justificado y sin perjuicio del nivel de garantía "alto" alcanzado por la solución Cartera en su conjunto. Para el uso de información de garantía procedente de otros sistemas o fuentes de certificación, se realizará un análisis de dependencia.

Por último, para garantizar un enfoque armonizado de la ciberseguridad y la evaluación de la

riesgos más críticos que puedan afectar a la provisión y funcionamiento de las Unidades Cartera, se define un registro de riesgos y amenazas, véase 7.4 Enfoque basado en riesgos y registro de riesgos. El Registro de Riesgos contiene riesgos y amenazas de alto nivel en relación con las Soluciones Cartera y el ecosistema, así como escenarios detallados de amenazas que se tendrán en cuenta a la hora de diseñar las Soluciones Cartera, independientemente de su arquitectura específica.

Como primer paso hacia la certificación de las soluciones Cartera en el marco de los sistemas nacionales, los Estados miembros asignarán un propietario del sistema, y diseñarán y pondrán en marcha el sistema. Como parte de este proceso, los organismos de certificación (OEC) serán acreditados para llevar a cabo las evaluaciones de conformidad de las soluciones Cartera con los requisitos del CIR 2024/2981 y el sistema nacional. A continuación, los Prestadores de Carteras solicitarán a uno o más OEC designados que evalúen y certifiquen la conformidad de su Solución de Cartera. El CAB evalúa y certifica la conformidad de la Solución Cartera si cumple los requisitos.

La Comisión Europea y ENISA apoyan a los Estados miembros en el diseño y aplicación de sistemas nacionales de certificación en el Grupo de Cooperación.

7.3 Certificación de las soluciones de Cartera según un sistema específico basado en CSA

Paralelamente al trabajo descrito anteriormente, se solicita a ENISA que elabore un esquema de certificación de ciberseguridad europeo específico para las Soluciones Cartera en el marco de la CSA. Una vez disponible, este esquema basado en la CSA sustituirá a los esquemas nacionales transitorios mencionados anteriormente para el requisito de ciberseguridad que cubre. Este esquema se basará en los esquemas nacionales disponibles, los requisitos armonizados e identificará cualquier requisito adicional relevante para la ciberseguridad. El sistema detallará los requisitos de ciberseguridad, identificará y establecerá normas y definirá el nivel de aseguramiento o seguridad objetivo para los componentes pertinentes de la solución de cartera.

El trabajo para desarrollar el esquema basado en la CSA sigue los hitos establecidos por la CSA y cuenta con el apoyo del Grupo de Trabajo Ad Hoc o "AHWG". Este grupo está compuesto por expertos seleccionados de organizaciones privadas y de la industria, con amplios conocimientos y experiencia en los ámbitos de la certificación de la ciberseguridad, las carteras digitales, la identificación electrónica y los servicios de

confianza. El primer paso es tener un esquema candidato listo para consulta pública y sometido a la opinión del Grupo Europeo de Certificación de Ciberseguridad o ECCG. El dictamen del ECCG sirve de asesoramiento para garantizar que el sistema candidato se ajusta a los objetivos, normas y requisitos reglamentarios de la UE en materia de ciberseguridad. Aunque el dictamen del ECCG no es vinculante, tendrá una influencia significativa, ya que refleja la experiencia colectiva de las autoridades nacionales de ciberseguridad,

con el objetivo de armonizar las prácticas de certificación de la ciberseguridad en todos los Estados miembros. Sobre la base de esta información, el sistema candidato podría . Una vez finalizado el dictamen del ECCG, el sistema se transformará en un nuevo Reglamento de Ejecución y se adoptará por el procedimiento de comitología.

Por último, también se pide a la ENISA que facilite la transición de los regímenes nacionales de certificación al régimen específico de certificación de la ciberseguridad en el marco de la CSA.

7.4 Enfoque basado en el riesgo y registro de riesgos

7.4.1 Introducción

En esta sección se detalla el enfoque para elaborar directrices armonizadas para el desarrollo de los sistemas nacionales de certificación transitorios. Además de los requisitos establecidos en el artículo 5c del Reglamento Europeo de Identidad Digital, se identificarán los riesgos y amenazas de ciberseguridad asociados a las Soluciones Cartera. En este caso, se prevé un enfoque basado en el riesgo como base para la certificación por parte de los Estados miembros, garantizando que las soluciones Cartera mantienen la confidencialidad, la disponibilidad y sólidas salvaguardias para la privacidad de los usuarios y la protección de datos. Esto se inspira en procesos conocidos, como el Reglamento General de Protección de Datos RGPD) y las correspondientes evaluaciones de impacto sobre la protección de datos (EIPD).

El enfoque basado en el riesgo establece un Registro de Riesgos común que contiene una lista exhaustiva pero no exhaustiva de riesgos y amenazas relacionados con la Solución Cartera. Estos riesgos y amenazas son independientes de la arquitectura y proporcionan una visión general de referencia de los riesgos y amenazas más críticos para las soluciones Cartera. Al adoptar este conjunto común de riesgos y amenazas, los sistemas nacionales de certificación transitoria alcanzarán un nivel básico de armonización.

El registro de riesgos será aplicado por los propietarios de sistemas, los Prestadores de Carteras y los Organismos de Certificación (OC). Al establecer sus sistemas de certificación, los propietarios de sistemas realizarán una de riesgos para perfeccionar y complementar los riesgos y amenazas enumerados en el registro con los específicos de su arquitectura, y estudiarán cómo tratar adecuadamente los riesgos y amenazas aplicables. Los Prestadores de Carteras complementarán la evaluación de riesgos del sistema para identificar los riesgos y amenazas específicos de su aplicación y propondrán medidas de mitigación adecuadas para su evaluación por el organismo de certificación.

7.4.2 Riesgos y amenazas de alto nivel

Lo que sigue es un extracto del [Registro de riesgos]. Para mantenerse en línea con el panorama de amenazas en continua evolución, el registro de riesgos se mantendrá y actualizará periódicamente en colaboración con el Grupo de Cooperación.

Riesgos y amenazas de alto nivel

R1 Creación o utilización de una identidad electrónica existente R2 Creación o utilización de una identidad electrónica falsa R3 Creación o utilización de atributos falsos R4 Robo de identidad R5 Robo de datos R6 Divulgación de datos R7 Manipulación de datos R8 Pérdida de datos R9 Transacción no autorizada R10 Manipulación de transacciones R11 Repudio R12 Divulgación de datos de transacciones R13 Interrupción del servicio R14 Vigilancia

Riesgos relacionados con el sistema

SR1 Vigilancia mayorista SR2 Daños a la reputación SR3 Incumplimiento legal Amenazas técnicas

TT1 Ataques físicos

1.1 Robo 1.2 Fuga de información 1.3 Manipulación TT2

Errores y desconfiguraciones

2.1 Errores cometidos al gestionar un sistema informático 2.2 Errores a nivel de aplicación o errores de uso 2.3 Errores en tiempo de desarrollo y desconfiguraciones del sistema

TT3 Utilización de fuentes poco fiables

3.1 Uso o configuración erróneos de los componentes de la Cartera

TT4 Fallos e interrupciones

4.1 Avería o disfunción de equipos, dispositivos o sistemas 4.2 Pérdida de recursos 4.3 Pérdida de servicios de apoyo

TT5 Acciones maliciosas

5.1 Interceptación de información 5.2 Phishing y spoofing 5.3 Repetición de mensajes 5.4 Ataque de fuerza bruta 5.5 Vulnerabilidades de software 5.6 Ataques a la cadena de suministro 5.7 Malware 5.8 Predicción de números aleatorios

7.4.3 Riesgos y medidas de mitigación analizados en el capítulo 6 del presente ARF.

7.4.3.1 Introducción

Esta sección discute brevemente algunos de los riesgos que se consideraron cuando se creó el modelo de confianza del Capítulo 6, junto con las mitigaciones para estos riesgos y los riesgos residuales que quedan después de estas mitigaciones. Esta sección no pretende ser un registro exhaustivo de riesgos para el ecosistema Cartera IDUE en su conjunto; para dicho registro, véase [Registro de Riesgos] y la Sección 7.4.2 anterior. Esta sección se limita al ámbito del ARF, es decir, la Unidad Cartera y sus interacciones con otras entidades del ecosistema, tal y como se representa en la Figura 11 del Capítulo 6.

7.4.3.2 Riesgos y medidas de mitigación en materia de confidencialidad, integridad y autenticidad

Dentro del ecosistema Cartera IDUE, se producen muchas interacciones entre entidades en las que una entidad solicita a otra que realice una tarea. Por ejemplo, un Usuario puede pedir a un Proveedor de DIP o a un Proveedor de Declaraciones que proporcione un DIP o una declaración a una Unidad Cartera, o una Parte usuaria (informada) puede pedir a un Usuario que presente atributos de una declaración en su Unidad Cartera. Para cualquiera de estas interacciones, se aplican los siguientes riesgos:

- Un atacante podría hacerse pasar por una de las entidades que interactúan. Por tanto, el receptor de un mensaje debe poder verificar la identidad del emisor, y viceversa. En otras palabras, es la autenticación mutua. Esta autenticación puede realizarse porque las entidades válidas del ecosistema Cartera IDUE son incluidas en una lista de confianza por los Estados miembros. Al comprobar la firma de un mensaje y verificar los certificados de clave pública asociados con un anclaje de confianza incluido en una lista de confianza, el receptor de un mensaje puede estar seguro de la identidad del remitente del mensaje.
- Los mensajes entre entidades podrían ser interceptados, lo que significa que podrían ser leídos por un atacante. Para mitigar este riesgo, los mensajes deben cifrarse para garantizar su confidencialidad.
- Los mensajes interceptados podrían ser modificados por un atacante. Para mitigar este riesgo, los mensajes deben estar autenticados, de modo que el receptor pueda verificar que proceden del remitente autenticado y que no han sido modificados.

7.4.3.3 Riesgos y medidas de mitigación relacionados con la manipulación de claves criptográficas y datos sensibles

Los mecanismos de autenticación y confidencialidad descritos en la sección anterior se basan en la seguridad de las claves criptográficas, especialmente las claves privadas y secretas. Si un atacante pueden obtener, utilizar o manipular estas claves, estos mecanismos de seguridad se romperían. Por lo tanto, todas las claves criptográficas son gestionadas por aplicaciones seguras dedicadas (WSCAs), que se ejecutan en hardware seguro (WSCDs), tal y como se describe en la Sección 4.3. La seguridad de los WSCD y las WSCA se garantiza mediante un proceso de certificación adecuado.

Estas medidas de mitigación se aplican a todas las entidades del ecosistema de Carteras IDUE que utilizan claves criptográficas, incluidas las Unidades de Cartera, los Proveedores de Carteras, los Proveedores de DIP y Proveedores de Declaraciones, los Proveedores de Listas de Confianza y las Autoridades de Certificación. Para las Partes usuarias e In- stancias de la Parte usuaria, estas medidas no son formalmente necesarias.

Los WSCDs y WSCAs en una Instancia Cartera también pueden ser utilizados para almacenar otros datos sensibles excepto claves criptográficas. En particular, podrían utilizarse para almacenar atributos de Usuario, de tal forma que los atacantes, incluyendo aplicaciones maliciosas que residan en el mismo dispositivo de Usuario que la Instancia Cartera, no puedan recuperar estos atributos. Esto es beneficioso para la privacidad del usuario.

7.4.3.4 Riesgos y medidas paliativas en relación con la autorización

En determinados casos, existe el riesgo de que una entidad legítima dentro del ecosistema Cartera IDUE intente realizar acciones más allá de su ámbito autorizado. Este riesgo afecta principalmente a dos tipos de entidades.

En primer lugar, un Prestador de DEA no cualificado puede intentar emitir declaraciones para las que carece de la autorización necesaria. Por ejemplo, un Prestador de servicios de certificación que no haya sido designado oficialmente por un Estado miembro u otra autoridad competente para expedir títulos puede intentar generar una declaración del tipo de título. Dentro del ecosistema de Carteras IDUE, este riesgo se limita a los Proveedores de DEA no cualificados, ya que se supone que los Proveedores de DIP, los Proveedores de DEA y los Proveedores de DEA-AAPP son intrínsecamente fiables en este contexto. Para más información, véase la sección 6.3.2.2.

Este riesgo se mitiga consultando el registro de Partes usuarias (informadas) a través de una API. Este registro, mantenido por el Estado miembro, contiene información exhaustiva sobre cada Parte usuaria (informada), lo que permite al sistema verificar la legitimidad del emisor y garantizar el cumplimiento de los requisitos reglamentarios.

En el contexto del Reglamento [Reglamento Europeo de Identidad Digital], el término Parte usuaria engloba tanto a los Prestadores de servicios de certificación como a las entidades que prestan servicios basados en declaraciones, garantizando un enfoque amplio y coherente de la confianza y la verificación dentro del ecosistema de Carteras IDUE.

En segundo lugar, una Parte usuaria en el ecosistema de Carteras IDUE puede intentar solicitar atributos de una Unidad de Cartera sin estar registrada o autorizada para ello. Este riesgo se mitiga principalmente con tres medidas:

1. **Divulgación selectiva y control del usuario** - Los formatos y protocolos de declaración especificados en [ISO/IEC 18013-5] y [SD-JWT VC] + [OpenID4VP] permiten la divulgación selectiva de atributos. Esto permite a una Parte usuaria (informada) especificar qué atributos de una declaración desea recibir y excluir otros, una característica conocida como *limitación de recopilación*. Además, la revelación selectiva garantiza que el usuario conserve el control sobre sus datos, ya que puede aprobar o denegar la presentación de los atributos solicitados. En la sección
   6.6.3.5 se .ofrecen más detalles sobre la divulgación selectiva y la aprobación del usuario
2. **Registro obligatorio por la Parte usuaria de los atributos solicitados** - El [Reglamento Europeo de Identidad Digital] exige que cada Parte usuaria registre los atributos que pretende solicitar a los usuarios. Según el CIR 2024/2982, estos registrados deben incluirse en un certificado de registro de la Parte usuaria, que la Unidad de Cartera utiliza para verificar la legitimidad de la solicitud e informar al usuario en consecuencia. Esta transparencia garantiza que los Usuarios puedan tomar una decisión informada sobre si aprobar o denegar la presentación de los atributos solicitados. En la sección 6.6.3.3 se .ofrecen más detalles sobre este requisito
3. **Cumplimiento de la política** de divulgación del proveedor de certificados - El [Reglamento Europeo de Identidad Digital] también establece que los proveedores de certificados pueden incluir una política de divulgación en sus declaraciones. Esta política puede incluir normas que regulen si el

Prestador de Certificados aprueba la presentación de esta declaración a una Parte usuaria (informada) autenticada. La Unidad Cartera evalúa esta política -si está presente- junto con los datos autenticados de la Parte usuaria, e informa al usuario del resultado. Este mecanismo ayuda al usuario a tomar una decisión bien informada sobre si aprueba o deniega la presentación de atributos. En los apartados 6.6.2.7 y 6.6.3.4 se .ofrece más información sobre la aplicación de la política de divulgación

7.4.3.5 Riesgos y medidas de mitigación relacionados con la privacidad de los usuarios

7.4.3.5.1 Vinculabilidad

La privacidad del usuario es una consideración clave en el diseño e implementación del ecosistema Cartera IDUE. Un aspecto importante de la privacidad es la disociabilidad. La desvinculación implica que, si un usuario presenta atributos de una declaración varias veces, las Partes usuarias receptoras no pueden vincular estas presentaciones separadas para concluir que se refieren al mismo usuario.

En el ecosistema de Carteras IDUE, los atributos se presentan en declaraciones electrónicas que contienen elementos únicos y fijos como valores hash, sales, claves públicas y firmas. Partes usuarias (informadas) malintencionadas podrían explotar estos valores para rastrear a los usuarios almacenándolos y comparándolos a través de múltiples transacciones, identificando patrones recurrentes. Esta amenaza a la privacidad, conocida como **vinculabilidad de la Parte** usuaria (informada), puede producirse dentro de una misma Parte usuaria (informada) o entre entidades coludidas.

Una amenaza similar para la privacidad surge cuando Partes usuarias coludidas comparten los valores únicos que obtuvieron en una declaración con un Proveedor de DIP o Proveedor de atestación malicioso. Esto permite al Proveedor de DIP o al Proveedor de Declaraciones rastrear la actividad del Usuario en múltiples servicios. En este caso, se denomina **vinculabilidad del Prestador de atestación**.

Este tema se trata con más detalle en el Documento de debate del Tema A.

7.4.3.5.2 Mitigación de la vinculabilidad de la Parte usuaria (informada)

Respecto a la mitigación de la vinculabilidad de la Parte usuaria (informada): Un Prestador de DIP o un Proveedor de Certificados de confianza puede mitigar totalmente la posibilidad de vinculación de la Parte usuaria emitiendo múltiples DIP o declaraciones a un mismo usuario. Las Unidades Cartera pueden utilizar estas declaraciones como declaraciones desechables (de un solo uso), lo que garantiza que las declaraciones nunca puedan ser vinculadas por Partes usuarias. El tema 10/23 del anexo 2 lo denomina "declaraciones de un solo uso" y exige que las soluciones Cartera admitan este método. También especifica cómo un Prestador de DIP o un Proveedor de atestaciones puede indicar que desea que una Unidad Cartera trate sus DIP o atestaciones de esta manera.

Sin embargo, el enfoque de "sólo una vez" aumenta la complejidad de la emisión y la sobrecarga de gestión. Por lo tanto, el Tema 10/23 también exige el apoyo a otra solución, en la que los DIP y los atestados son válidos sólo durante un tiempo limitado. Esto limita la cantidad de DIP y declaraciones que deben emitirse, pero sólo mitiga parcialmente la vinculabilidad de la Parte usuaria (informada). El tema 10/23 lo denomina "declaraciones por tiempo limitado".

Además, el Tema 10/23 describe otros dos enfoques, que son opcionalmente soportados por las Unidades Cartera, a saber:

- El Prestador de Servicios de Certificación emite declaraciones por lotes para la Unidad Cartera. A continuación, la Unidad Cartera utiliza las declaraciones de un lote en un orden aleatorio, hasta que ha presentado todas las declaraciones del lote una vez. A continuación, "restablece" el lote y comienza a utilizarlos de nuevo en un orden aleatorio. El Tema 10/23 lo denomina "declaraciones por lotes rotatorios".
- la Unidad Cartera presentará declaraciones diferentes a las distintas Partes usuarias. Sin embargo, en caso de que una Parte usuaria solicite atributos de esta declaración varias veces, la Unidad de Cartera presentará la misma declaración a esta Parte usuaria cada vez. El tema 10/23 lo denomina "declaraciones por Parte usuaria".

Además, las medidas organizativas y coercitivas pueden ayudar a disuadir a las Partes usuarias de confabularse y seguir a los usuarios. En particular, se revocarán los certificados de acceso de las Partes usuarias infractoras, lo que les impedirá seguir interactuando con las Unidades de Cartera.

7.4.3.5.3 Pruebas de conocimiento cero

La vinculabilidad del Prestador de servicios de certificación no puede eliminarse por completo cuando se utilizan formatos de declaración basados en hashes con sal. La única solución viable es adoptar las Pruebas de Conocimiento Cero (ZKP) como mecanismo de verificación en lugar de basarse en hashes de atributos con sal. Sin embargo, la integración de las ZKP en el ecosistema Cartera IDUE sigue siendo objeto de debate y desarrollo debido a la complejidad de implementar soluciones ZKP en hardware seguro y a la falta de soporte en el hardware seguro actualmente disponible (WSCDs). Al igual que en el caso de la vinculabilidad de la Parte usuaria, las medidas organizativas y coercitivas pueden contribuir a disuadir a los Prestadores de servicios de certificación de la colusión y el seguimiento de los usuarios. Además, muchos Prestadores de servicios de certificación están sujetos a auditorías periódicas, lo que facilita la detección de la colusión y el seguimiento en comparación con las Partes usuarias (informadas).

Los mecanismos de prueba de conocimiento cero (ZKP) para verificar la información personal son muy prometedores y esenciales para garantizar la privacidad en diversos casos de uso. Permiten a los usuarios demostrar afirmaciones como "soy mayor de 18 años" sin revelar ningún dato personal, lo que ofrece una solución sólida para la autenticación y verificación que preserva la privacidad.

Un área clave de desarrollo es la verificación de la edad, donde la Comisión Europea está explorando y probando activamente soluciones basadas en ZKP. Los resultados de esta iniciativa podrían allanar el camino para la adopción de ZKP en el ecosistema de Cartera IDUE, reforzando aún más la protección de la privacidad en futuras implementaciones.

El documento de debate para el tema G Pruebas de conocimiento cero) presenta las propiedades de privacidad (deseadas) de los esquemas de prueba de conocimiento cero. Presenta las principales familias de esquemas de prueba de conocimiento-cero y ofrece una visión general de soluciones representativas. Finalmente, se discuten temas relacionados con la integración de esquemas de prueba de conocimientocero en el ecosistema de Cartera IDUE.

8 Desarrollo de documentos

8.1 Publicación

Este documento está a disposición del público en https://github.com/eu-digital-identity-wallet/e udi-docarchitecture-and-reference-framework (repositorio GitHub), donde se actualizará periódicamente.

8.2 Contribución

Valoramos sus comentarios y le animamos a que comparta con nosotros cualquier idea, sugerencia o preocupación que pueda tener en relación con este documento.

8.2.1 Proporcionar comentarios

Para hacernos llegar sus comentarios sobre este documento, visite nuestro repositorio de GitHub. Para ello, vaya a la pestaña "Temas" y envíe un nuevo tema o comente los ya existentes. ha detectado un error tipográfico, tiene alguna sugerencia para aclarar una sección o quiere proponer un nuevo tema para su inclusión, agradeceremos sus comentarios.

8.2.1.1 Directrices para añadir incidencias al repositorio de Github

Cuando añada incidencias al repositorio de Github, siga estas directrices generales:

- Utiliza **títulos claros y descriptivos** para resumir de forma concisa el problema o la tarea. Esto ayuda a los demás a entender rápidamente la cuestión de un vistazo.
- **Describa detalladamente el problema**, incluyendo el contexto y la información de fondo pertinentes. La descripción debe ser lo suficientemente completa como para que otros puedan entender el problema y tomar las medidas adecuadas.
- Utilice una o varias de las siguientes **etiquetas** para clasificar las incidencias. Las etiquetas ayudan a organizar y priorizar las incidencias, facilitando la gestión del repositorio.

Etiqueta	Descripción
Aclaraciones sobre el contenido	Plantee cuestiones solicitando aclaraciones sobre contenidos específicos del documento. Puede tratarse de explicaciones de conceptos, definiciones de términos o ejemplos para ilustrar determinados puntos.

Sugerencias de mejora	Proponga sugerencias para mejorar la claridad, exhaustividad o precisión del documento. Puede tratarse de reestructurar secciones, añadir ejemplos o facilitar información adicional.

Etiqueta	**Descripción**
Errores y correcciones	Identifique errores como erratas, errores gramaticales o imprecisiones factuales en el documento y sugiera correcciones.
Compatibilidad e integración	Cuestiones relacionadas con el modo en que el documento se integra con otros sistemas o tecnologías, garantizando la compatibilidad con distintas plataformas o marcos.
Solicitudes de mejora	Solicite que se añadan nuevas funciones, secciones o contenidos al documento para mejorar su utilidad o relevancia.
Formato y estilo	Comentarios sobre el aspecto visual, la organización y la coherencia del formato del documento.
Normas de documentación	Debates sobre el cumplimiento de las normas, convenciones o directrices de documentación.
Licencia y cuestiones jurídicas	Preguntas o dudas relacionadas con la licencia del documento, los derechos de uso, los requisitos de atribución o las implicaciones legales para colaboradores y usuarios.
Aclaraciones técnicas	Plantee cuestiones que pidan aclaraciones sobre contenidos técnicos específicos del documento.

- **Adjunte** archivos relevantes, capturas de pantalla o enlaces a recursos adicionales que proporcionen contexto o ayuden a resolver el problema. Esto puede incluir referencias a documentación o debates relacionados.

- **Siga el protocolo de incidencias** realizando una búsqueda para comprobar si la incidencia ya ha sido notificada antes de crear nueva. Esto ayuda a evitar la duplicación de incidencias.

8.2.1.2 Directrices para debatir problemas existentes en el repositorio de GitHub

Cuando hables de problemas existentes en el repositorio de Github, sigue estas directrices generales:

- **Comuníquese con respeto y cortesía** hacia los demás colaboradores, mantenga un tono profesional y evite utilizar un lenguaje que pueda interpretarse como conflictivo o incendiario.
- Proporcione **contexto e información de fondo** para ayudar a los demás a entender su punto de vista. Explique los motivos de sus comentarios.
- Comunique sus intenciones y motivaciones detrás de sus comentarios o sugerencias para **evitar malentendidos**.
- Mantenga **los debates centrados en los aspectos técnicos del** asunto en .
- Proporcione **comentarios y sugerencias constructivas** de útil y solidaria. En lugar de limitarse a señalar los problemas, ofrezca soluciones o enfoques alternativos para abordar la cuestión de forma positiva.
- Aborde los debates con una **mentalidad de colaboración y resolución de problemas**.
- Esté **abierto a diferentes perspectivas**, ya que los colaboradores pueden tener diferentes puntos de vista, experiencias y niveles de conocimientos.
- Contribuir a crear un **ambiente comunitario positivo y acogedor**.

8.2.2 Gestión de incidencias y Pull Requests

Nuestro equipo se compromete a gestionar las incidencias y pull requests relacionadas con este documento de forma transparente y eficiente para garantizar que todos los comentarios se abordan con prontitud y eficacia. A continuación te explicamos cómo gestionamos las incidencias y pull requests para establecer las expectativas adecuadas:

- Gestión de problemas: Cuando se envía una incidencia, nuestro equipo la revisa y prioriza en función de su relevancia e impacto. Le mantendremos informado del estado de su incidencia y le proporcionaremos actualizaciones a medida que avance. Una vez resuelta, cerraremos la incidencia e incorporaremos los cambios necesarios al documento.
- Gestión de solicitudes: Si envía una solicitud de extracción con cambios o mejoras propuestos para el , nuestro equipo la revisará detenidamente y le proporcionará comentarios y sugerencias para su perfeccionamiento. Colaboraremos con usted para asegurarnos de que su contribución se ajusta a

los objetivos del documento y mantiene la coherencia y la calidad. Una vez aprobados los cambios, los incorporaremos al documento y reconoceremos su contribución.

Sus comentarios y contribuciones son esenciales para ayudarnos a mantener la calidad y pertinencia de este . Valoramos su participación y nos esforzamos por crear un entorno de colaboración en el que se valoren y reconozcan las contribuciones de todos.

8.3 Versionado de documentos

Para evitar problemas de interoperabilidad y que los cambios en el ARF pasen desapercibidos, se utilizará un sistema de control de versiones y el siguiente esquema semántico de versiones (https://semver.org) para el ARF.

El documento ARF se publicará con un formato de versión normalizado, *MA- JOR.MINOR.PATCH*, donde:

La versión **MAJOR** se incrementa (es decir, nueva versión), cuando el documento ARF ha *sufrido cambios significativos, por ejemplo introduciendo algunos cambios de ruptura en* la arquitectura,

La versión **MINOR** se incrementa cuando se ha añadido nueva información al *documento o se ha eliminado información del documento, y

La versión **PATCH** se incrementa cuando se han realizado cambios menores (por ejemplo, arreglar *typos).

9 Referencias

Para las referencias sin fecha, se aplica la última versión disponible.

Artículo Referencia	Nombre estándar/detalles
[2015/1505]	DECISIÓN DE EJECUCIÓN DE LA COMISIÓN (UE) 2015/1505 de 8 de septiembre de 2015 por el que se establecen especificaciones técnicas y formatos relativos a las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Artículo Referencia	Nombre estándar/detalles

[Regulación europea de la identidad digital]	Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del Marco Europeo de Identidad Digital.
[Registro de riesgos]	
[CIR 2024/2977]	Reglamento (UE) 2024/2981, Anexo I de 28 de noviembre de 2024 por el que se establecen las normas de aplicación del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la certificación de las Carteras de Identidad Digital Europeas.
[CIR 2024/2979]	Reglamento de Ejecución 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 las personas y a las declaraciones electrónicas de Atributos expedidas a las Carteras de Identidad Digital Europeas.
[CIR 2024/2980]	Reglamento de Ejecución 2024/2979 de la Comisión, de 28 de noviembre de 2024, por el que se establecen las 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 de Identidad Digital Europeas.
[CIR 2024/2981]	Reglamento de Ejecución 2024/2980 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las notificaciones a la Comisión relativas al ecosistema de la Cartera de Identidad Digital Europea.
[CIR 2024/2982]	Reglamento (UE) 2024/2981, de 28 de noviembre de 2024, por el que se establecen las disposiciones de aplicación del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la certificación de las Carteras de Identidad Digital Europeas.
[ISO/IEC 18013-5]	Reglamento de Ejecución 2024/2982 de la Comisión, de 28 de noviembre de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo en lo relativo a los protocolos e interfaces que debe admitir el Marco Europeo de Identidad Digital. ISO/IEC 18013-5, Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application (Identificación personal - Permiso de conducción conforme a la norma ISO - Parte 5: Aplicación del Carné de Conducir Móvil (CCm))

Referencia	Artículo Nombre estándar/detalles
[ISO/IEC 18013-7]	ISO/IEC 18013-7,)Personal identification - ISO-compliant driving licence - Part 7: Mobile driving licence (mDL) add-on functions (Identificación personal - Carné de Conducir Móvil
[ISO 3166-1]	(CCm) ISO 3166-1: Códigos para la representación de los nombres de países y sus subdivisiones -
[ISO 3166-2]	Parte 1. Códigos de país: alfa-2 países: Códigos de país: país alfa-2 ISO 3166-2:2020: Códigos para la representación de nombres de países y sus subdivisiones - [ETSI TS Parte 2: Código de subdivisión de país.
119 612]	ETSI TS 119 612: Firmas e infraestructuras electrónicas (ESI); listas de confianza
[ETSI TS 119 431-1]	ETSI TS 119 431-1 - Firmas electrónicas e infraestructuras (ESI); Política y requisitos de seguridad para proveedores de servicios de confianza; Parte 1: Componentes de servicio [ETSI TS 119 TSP que operan un QSCD / SCDev remoto.
431-2]	ETSI TS 119 431-2 - Firmas e Infraestructuras Electrónicas (ESI); Política y requisitos de seguridad para proveedores de servicios de confianza; Parte 2: Componentes de servicio TSP que soportan la creación de firma digital AdES [ETSI TS
119 432]	ETSI TS 119 432 - Firmas e Infraestructuras Electrónicas (ESI); Protocolos para la creación remota de firmas digitales
[ETSI EN 319 132-1]	ETSI EN 319 132-1 - Firmas e Infraestructuras Electrónicas (ESI); Firmas digitales XAdES; Parte 1: Bloques de construcción y firmas de base XAdES (XAdES)
[ETSI TS 119 182-1]	ETSI TS 119 182-1 - Firmas e Infraestructuras Electrónicas (ESI); Firmas digitales JAdES; Parte 1: Bloques de construcción y firmas base JAdES
[ETSI EN 319 122-1]	ETSI EN 319 122-1 - Firmas e Infraestructuras Electrónicas (ESI); Firmas digitales CAdES; Parte 1: Bloques de construcción y firmas base CAdES
[ETSI EN 319 162-1]	ETSI EN 319 162-1 - Firmas e Infraestructuras Electrónicas (ESI); Contenedores de Firma Asociados (ASiC); Parte 1: Building blocks y contenedores base ASiC

ETSI EN 319 142-1 - Firmas e Infraestructuras Electrónicas (ESI); Firmas digitales PAdES; Parte 1: Bloques de construcción y firmas base PAdES

[ETSI EN 319 142]

Artículo Referencia	Nombre estándar/detalles
[CEN EN 241-1]	CEN EN 419 241-1 - Sistemas de confianza que admiten firma de servidor - Parte 1. Requisitos generales de seguridad del sistema Requisitos generales de seguridad del sistema
[SD-JWT VC]	Credenciales verificables basadas en SD-JWT (SD-JWT VC). Disponible en: https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/
[RFC 2119]	RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels. S. Bradner, marzo de 1997.
[RFC 3339]	RFC 3339 - Fecha y hora en Internet: Timestamps, G. Klyne et al., julio de 2002 [RFC 4122]
	RFC 9562 - Universally Unique IDentifiers (UUIDs), P. Leach et al., Mayo 2024
[RFC 5280]	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Kooper et al., Mayo 2008
[RFC 3647]	RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokhani et al., noviembre de 2003
[RFC 7519]	RFC 7519 - Token web JSON (JWT), M. Jones y otros, mayo de 2015.
[RFC 8259]	RFC 8259 - El formato de intercambio de datos JavaScript Object Notation (JSON), T. Bray, Ed., diciembre de 2017
[RFC 8610]	RFC 8610 - Lenguaje conciso de definición de datos (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures, H. Birkholz y otros, junio de 2019.
[RFC 8943]	RFC 8943 - Concise Binary Object Representation (CBOR) Tags for Date, M. Jones et al., noviembre de 2020
[RFC 8949]	RFC 8949 - Representación concisa de objetos binarios (CBOR), C. Bormann et al., Diciembre de 2020
[API DEL CSC]	Cloud Signature Consortium API Specification v2.0, 20 de abril de 2023
[GP OMAPI]	GPD_SPE_075 Especificación de API móvil abierta, v3.3, julio de 2018, GlobalPlatform [GP
CS]	GPC_SPE_034 Especificación de la tarjeta, v2.3.1, marzo de 2018, GlobalPlatform
[GSMA SAM]	GSMA Secured Applications for Mobile, v1.1, 03 de noviembre de 2023, GSM Association

Artículo Referencia	Nombre estándar/detalles
[W3C VCDM v1.1]	Sporny, M., Longley, D. y D. Chadwick, "Verifiable Credentials Data Model 1.1", Recomendación del W3C, 03 de marzo de 2022.
[W3C VCDM v2.0]	Sporny, M. *et al,* "Verifiable Credentials Data Model v2.0", W3C Candidate Recommendations Draft, 16 de abril de 2024.
[W3C API de credenciales digitales].	Cáceres, M., Cappalli, T., Goto, S. *et al,* "API de credenciales digitales"
[W3C WebAuthn]	Autenticación web, una API para acceder a credenciales de clave pública de nivel 2, Recomendación del W3C
[CTAP]	Client to Authenticator Protocol (CTAP) Review Draft, 21 de marzo de 2023. Disponible: https://fidoalliance.org/specs/fido-v2.2-rd-20230321/fido-client-to- authenticator-protocolv2.2-rd-20230321.html

[OpenID4VCI] Lodderstedt, T. et al., "OpenID for Verifiable Credential Issuance", OpenID Foundation.

[OpenID4VP] Terbu, O. y otros, "OpenID Connect for Verifiable Presentations", OpenID Foundation.

[OIDC] Sakimura, N. y otros, "OpenID Connect Core 1.0", OpenID Foundation. Disponible: https://openid.net/specs/openid-connect-core-1_0.html

[EKYC] Lodderstedt, T. y otros, "OpenID Connect for Identity Assurance Claims Registration 1.0", OpenID Foundation. Disponible: https://openid.net/specs/openid-connect-4-ida-claims-1_0-final.html

[EKYC Esquema] Lodderstedt, T. y otros, "OpenID Identity Assurance Schema Definition 1.0", OpenID Foundation. Disponible: https://openid.net/specs/openid-ida-verified-claims-1_0-final.html

[HAIP] Yasuda, K. et al, "OpenID4VC High Assurance Interoperability Profile", OpenId Foundation.

[IANA-JWT-Claims] Registro de reclamaciones de tokens web JSON de la IANA. Disponible: https://www.iana.org/assignments/jwt/jwt.xhtml

Artículo Referencia	Nombre estándar/detalles

[Tema 6] Anexo 2 - Autenticación de la Parte usuaria y aprobación del usuario

[Tema 7] Anexo 2 - Revocación de la declaración y comprobación de la revocación

[Tema 9] Anexo 2 - Declaración de la Unidad Cartera

[Tema 10]	Anexo 2 - Emisión de un DIP o declaración a una Unidad Cartera
[Tema 11]	Anexo 2 - Seudónimos
[Tema 12]	Anexo 2 - Directrices de elaboración de declaraciones
[Tema 16]	Anexo 2 - Firma de documentos con una unidad Cartera
[Tema 18]	Anexo 2 - Presentaciones combinadas de atributos
[Tema 19]	Anexo 2 - Requisitos de navegación de los usuarios (Registros del cuadro de mandos para la transparencia)
[Tema 23]	Anexo 2 - Emisión de DIP y emisión de (Q)DEA
[Tema 25]	Anexo 2 - Definición unificada y vocabularios controlados para atributos
[Tema 26]	Anexo 2 - Catálogo de declaraciones
[Tema 27]	Anexo 2 - Registro de Prestadores de DIP, Prestadores de DEA-CA, DEA-AAPP y DEA-AAPP (no cualificadas), y Partes usuarias (informadas)
[Tema 30]	Anexo 2 - Interacción entre unidades Cartera
[Tema 31]	Anexo 2 - Notificación y publicación del Proveedor de DIP, el Proveedor de Carteras, el Proveedor de Declaraciones y la Autoridad de Certificación de Acceso
[Tema 33]	Anexo 2 - Copia de seguridad y restauración de la unidad Cartera
[Tema 34]	Anexo 2 - Migrar a otra solución Cartera
[Tema 37]	Anexo 2 - FEC - Firma remota - Requisitos técnicos
[Tema 38]	Anexo 2 - Revocación de la Unidad Cartera
[Tema 42]	Anexo 2 - Requisitos para que los QTSP accedan a fuentes auténticas
[Tema 43]	Anexo 2 - Políticas de divulgación incorporadas
[Tema 44]	Anexo 2 - Certificados de registro de Parte usuaria (informada)
[Tema 48]	Anexo 2 - Modelo para solicitar la supresión de datos a las Partes usuarias (informadas)

Artículo Referencia	**Nombre estándar/detalles**
[Tema 50]	Anexo 2 - Plan para notificar la solicitud ilegal o sospechosa de datos
[Tema 51]	Anexo 2 - DIP o supresión de declaración
[Tema 52]	Anexo 2 - Parte usuaria (informada) intermediaria

10 Anexos

- Definiciones - Anexo 1
- Requisitos técnicos de alto nivel - Anexo 2
- Directrices de elaboración - Anexo 3:
  - Directrices de elaboración del DIP - Anexo 3.1
  - Directrices de elaboración del Carné de Conducir Móvil (CCm) - Anexo 3.2
- Planos de servicios - Anexo 4:
  - Inicialización y activación de Blueprint - Anexo 4.1
  - Blueprint Identificación y autenticación en línea - Anexo 4.2
  - Plano de Expedición del Carné de Conducir Móvil (CCm) - Anexo 4.3
  - Plano de Presentación del Carné de Conducir Móvil (CCm) - Anexo 4.4
  - Plano de Presentación del Carné de Conducir Móvil (CCm) - Anexo 4.5
  - Blueprint FEC remoto - Creación de una firma para autenticación / autorización Anexo 4.6
  - Blueprint Remote FEC - Matriculación - Anexo 4.7
  - Plano FEC Remoto - Creación de una firma canalizada por una Unidad Cartera - Anexo 4.8
  - Blueprint FEC Remoto - Creación de una firma canalizada por Parte usuaria (informada) - Anexo 4.9
  - Blueprint FEC - Ver historial de firmas - Anexo 4.10
  - Plan Local FEC - Matriculación - Anexo 4.11 – Plan Local FEC - Creación de una firma - Anexo 4.12
- Guías de diseño - Anexo 5:
  - Guía de diseño de la Unidad Cartera - Anexo 5.1
  - Guía de diseño de la Unidad Cartera - escenarios de intercambio de datos - Anexo 5.2