La Caja de herramientas Común de la Unión para un enfoque coordinado hacia un Marco Europeo de Identidad Digital

Arquitectura y marco de referencia de la cartera europea de identidad digital

Abril de 2023

Versión 1.1.0

VERSIÓN DEL DOCUMENTO

VERSIÓN	FECHA[1]	CAMBIOS
1.0.0	26 de enero de 2023	Primera versión
1.1.0	20 de abril de 2023	Adición de planos de servicios para casos de uso en: - Identificación y autenticación para acceder a los servicios en línea, y - permiso de conducción móvil

[1] La fecha de adopción por el Grupo de Expertos eIDAS

Contenido

1. Introducción

1.1. Contexto

El 3 de junio de 2021, la Comisión Europea adoptó una Recomendación[2] en la que se pide a los Estados miembros que trabajen en el desarrollo de una caja de herramientas que incluya una arquitectura técnica y un marco de referencia (en lo sucesivo, el ARF, por su designación en inglés "Architecture and Reference Framework"), 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 de la propuesta de Marco Europeo de Identidad Digital[3] sin que el proceso de elaboración de la caja de herramientas interfiera o prejuzgue el proceso legislativo.

La Recomendación prevé que la caja de herramientas sea desarrollada por expertos de los Estados miembros en el Grupo de Expertos eIDAS[4]en estrecha coordinación con la Comisión y, cuando sea pertinente para el funcionamiento de la infraestructura de la Cartera de Identidad Digital de la Unión Europea (IDUE), con otras partes interesadas de los sectores público y privado.

Siguiendo el calendario indicativo establecido en la Recomendación, el 30 de septiembre de 2021 se acordaron un proceso y unos procedimientos de trabajo que se debatieron en un documento oficioso sobre una descripción de alto nivel del ecosistema Cartera IDUE, propuesto por la Comisión.

Sobre esta base, entre octubre y diciembre de 2021 se definió un esquema que proporcionaba una descripción más detallada del concepto de cartera IDUE, sus funcionalidades y aspectos de seguridad, así como de varios casos de uso básicos. Ese trabajo dio lugar al Esbozo del ARF, adoptado por el Grupo de Expertos eIDAS en febrero de 2022. El esquema se publicó en Futurium[5] para recabar la opinión del público. Cuando se cerró el periodo de comentarios el 15 de abril de 2022, 36 partes interesadas habían enviado sus comentarios sobre el Esbozo.

Desde entonces, el Grupo de Expertos eIDAS ha seguido desarrollando los conceptos y especificaciones del Marco Europeo de Identidad Digital sobre la base de la propuesta de

[2] RECOMENDACIÓN DE LA COMISIÓN (UE) C(2021) 3968 final 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.

[3] Todas las referencias en el documento a la revisión del Reglamento eIDAS deben entenderse hechas a la propuesta de la Comisión de 3 de junio de 2021, salvo indicación en contrario. Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento de un marco para la identidad digital europea, COM(2021) 281 final de 3.6.2021

[4] https://ec.europa.eu/transparency/expert-groups-register/screen/expert groups/consult?do=detalle_grupo.groupDetail&groupID=3032

[5] https://futurium.ec.europa.eu/en/digital-identity/toolbox/architecture-and-reference-framework-outline

revisión del Reglamento EIDAS de la Comisión[6] y seguirá haciéndolo hasta que concluyan las negociaciones legislativas y se adopten los actos de ejecución..

El Grupo de Expertos eIDAS adoptó el presente documento el 20 de abril de 2023.

1.2. Sobre este documento

1.2.1. Autoría y Licencia

Este documento es el resultado del trabajo del Grupo de Expertos eIDAS (eIDAS Expert Group) (E03032)[7] cuya última reunión tuvo lugar el 20/03/2023 (a los efectos de esta versión del documento).

La versión original en inglés de este documento mantenida en una herramienta que promueve la cooperación y contribuciones de diferentes autores está disponible en https://code.europa.eu/eudi/architecture-and-reference-framework

Esta forma de gestionar el documento hace recomendable recurrir a esa URL para acceder a las versiones más actualizadas del documento en inglés.

La licencia respecto a la Propiedad Intelectual del documento es Creative Commons "Atribución 4.0 Internacional (CC BY 4.0)" https://code.europa.eu/eudi/architecture-and-reference-framework/-/blob/main/LICENSE que permite:

- Compartir — copiar y redistribuir el material en cualquier medio o formato
- Adaptar — remezclar, transformar y construir a partir del material para cualquier propósito, incluso comercialmente.

Bajo los siguientes términos:

- Atribución — Usted debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licencian

1.2.2. Traducción y Licencia.

La versión en español la ha realizado **Julián Inza**, Presidente de EADTRUST, un Prestador Cualificado de Servicios de Confianza radicado en Madrid (España) con página web https://eadtrust.eu y se ha finalizado el 11 de septiembre de 2023, varias semanas días después

[6] Todas las referencias del documento a la revisión del Reglamento eIDAS deben entenderse hechas a la propuesta de la Comisión de 3 de junio de 2021, salvo que se indique lo contrario.
[7] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3032

de que se publicara la versión original en inglés en la página web de Github https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

El documento se publica con la misma licencia Creative Commons "Atribución 4.0 Internacional (CC BY 4.0) por lo que surte efectos el enlace indicado anteriormente.

Cualquier obra derivada debe indicar que se ha desarrollado a partir de la traducción realizada por **Julián Inza**, Presidente de EADTRUST European Agency of Digital Trust, S.L, un Prestador Cualificado de Servicios de Confianza radicado en Madrid (España) con página web https://eadtrust.eu

1.2.3. Finalidad de este documento.

El objetivo del documento es proporcionar todas las especificaciones necesarias para desarrollar una solución interoperable de cartera IDUE basada en normas y prácticas comunes. El documento presenta un estado de los trabajos en curso del Grupo de Expertos eIDAS y no implica ningún acuerdo formal sobre su contenido o la propuesta de revisión del Reglamento EIDAS. 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. Una vez completado, el documento describirá una Arquitectura y un Marco de Referencia completos que abarcarán todas las especificaciones necesarias para implantar una Solución Europea de Cartera de Identidad Digital.

Mientras que los capítulos 2-4 y 7-8 son descriptivos, los capítulos 5 y 6 especifican los requisitos para los prestadores de DIP/PID y TE(C)A/(Q)EAA y los implementadores de soluciones de Cartera IDUE. Las expresiones imperativas en mayúsculas en el documento se utilizan de acuerdo con la norma técnica RFC 2119.

El documento en sí no tiene valor legal y no prejuzgará el proceso legislativo en curso y los requisitos legales obligatorios finales para las carteras europeas de identidad digital. El ARF se ajustará al resultado de las negociaciones legislativas de la propuesta de Marco Europeo de Identidad Digital. Sólo serán obligatorios el Reglamento Marco Europeo de Identidad Digital finalmente adoptado y los actos de ejecución y delegados adoptados con arreglo a dicha base jurídica.

1.3. Uso de este documento

Este documento está destinado principalmente a ser utilizado por la Comisión Europea que desarrolla una implementación de referencia de una Cartera IDUE y los consorcios que ejecutan proyectos piloto enfocados en el uso de la implementación de referencia en el contexto de "Large Scale Pilots" (Pilotos a Gran Escala). La experiencia adquirida en la aplicación de esta

especificación puede dar lugar a mejoras del presente documento, de conformidad con el capítulo 8.

1.3.1. La implementación de referencia de una cartera IDUE

La Comisión proporcionará una implementación de referencia de la cartera IDUE en un formato móvil[8]. El código de la implementación de referencia de Cartera IDUE se proporcionará como software de fuentes abiertas para su reutilización por los implementadores de toda Europa. Los primeros implementadores serán los proyectos seleccionados para llevar a cabo los Large Scale Pilots (LSPs), tras una convocatoria de propuestas semejante a una licitación. Los proyectos LSP participarán en el desarrollo de la implementación de referencia de una Cartera IDUE. La Comisión también prestará inicialmente los servicios centrales necesarios para el funcionamiento de la implementación de referencia de la Cartera IDUE.

La Comisión se propone utilizar el ARF para desarrollar la aplicación de referencia de la Cartera IDUE.

1.3.2. Orientaciones para los pilotos a gran escala (Large Scale Pilots LSP)

Para apoyar el desarrollo de una implementación de referencia de una cartera IDUE y probar su uso a través de diferentes casos de uso prioritarios en proyectos piloto, la Comisión lanzó una convocatoria de propuestas el 22 de febrero de 2022 en el marco del Programa Europa Digital para acoger casos de uso a gran escala para la cartera IDUE.

El objetivo de la convocatoria Large Scale Pilots (LSP) es cofinanciar proyectos piloto que hagan uso de la cartera IDUE basada en una implementación de referencia del software de cartera IDUE, teniendo en cuenta las especificidades del proyecto, los sistemas existentes de Identidad Digital notificados (como el DNIe en el caso de España) y los desarrollos nacionales de sistemas de Cartera y las situaciones de implementación, en torno a los diferentes casos de uso transfronterizos que implican a partes interesadas tanto públicas como privadas.

El ARF será utilizado por los LSP para informar y guiar el diseño de sistemas de los pilotos y el desarrollo de la arquitectura junto con la publicación de la implementación de referencia.

Se espera que los LSP aporten sus comentarios sobre el ARF a medida que desarrollen e interactúen con los servicios de las partes de confianza, los proveedores cualificados o no

[8] Actualmente está prevista una primera versión para el segundo trimestre de 2023, a la que seguirán otras.

cualificados de testimonios electrónicos de atributos TE(C)A/(Q)EAA, los proveedores de datos de identificación de personas (DIP/PID) y los usuarios en transacciones significativas según los casos de uso propuestos.

2. Definiciones

Además del artículo 3 de la propuesta de modificación del texto legal del Reglamento EIDAS (anterior Reglamento UE 910/2014) se ofrecen las siguientes definiciones para destacar las más relevantes para la Arquitectura y el Marco de Referencia o para introducir términos adicionales no definidos en el citado texto legal (señalados con un *).

Atributo	**Rasgo, característica o cualidad de una persona física o jurídica o de una entidad, en forma electrónica. - *Propuesta de modificación del Reglamento eIDAS***
Fuente auténtica	**Repositorio o sistema, mantenido bajo la responsabilidad de un organismo del sector público o una entidad privada, que contiene atributos sobre una persona física o jurídica y se considera la fuente primaria de esa información o se reconoce como auténtica en la legislación nacional. - *Propuesta de modificación del Reglamento eIDAS***
Testimonio electrónico de atributos (TEA)	*En inglés: Electronic Attestation of Attributes (EAA)* **Un testimonio en formato electrónico que permite la autenticación de atributos - *Propuesta de modificación del Reglamento eIDAS***
*Emisor**	**Un prestador que informa sobre datos de identificación de persona (DIP/PID) o un prestador de servicios de confianza (cualificado o no) que emite atributos TE(C)A/(Q)EAA. En el caso de la cartera IDUE, puede haber varios emisores de DIP/PID y de TE(C)A/(Q)EAA.**
Organismos nacionales de acreditación (ONA).*	*En inglés: National Accreditation Bodies (NAB)* **Los Organismos Nacionales de Acreditación (ONA) con arreglo al Reglamento (CE) nº 765/2008 son los organismos de los Estados miembros que realizan la acreditación de Organismos de Evaluación de Conformaidad con autoridad derivada del Estado.**
Datos de identificación de la persona (DIP)	*En inglés: Person Identification Data (PID)* **Conjunto de datos que permiten establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica - *Reglamento eIDAS*.**
*Proveedor de datos de identificación de personas**	**Estado miembro o entidad jurídica que proporciona datos de identificación de la persona a los usuarios como fuente primaria.**

Infraestructura de clave pública (PKI).*	*En inglés, Public Key Infraestructure (PKI)* **Denota sistemas, software y protocolos de comunicación que utilizan los componentes de una Cartera IDUE para distribuir, gestionar y controlar claves públicas. Una PKI entrega claves públicas embebidas en certificados y gestiona su confiabilidad respondiendo sobre la vigencia de los certificados que ha emitido.**
Prestador de Testimonios electrónicos cualificadas de atributos	**Proveedor cualificado de servicios de confianza que expide testimonios electrónicos de atributos, y que cumple los requisitos establecidos en el anexo V. - *Propuesta de modificación del Reglamento eIDAS***
Dispositivo Cualificado de Creación de Firma (DCCF)	*En inglés, Qualified Signature creation Device (QSCD)* **Software o hardware configurado para crear firmas electrónicas que cumpla los requisitos establecidos en el anexo II de la propuesta de modificación del Reglamento eIDAS. *Reglamento eIDAS y propuesta de modificación del Reglamento eIDAS***
Prestador cualificado de servicios de confianza (PCSC)	*En inglés, Qualified Trust Service Provider (PCSC)* **Un proveedor de servicios de confianza que presta uno o varios servicios de confianza cualificados cuando el organismo de supervisión le haya concedido la condición de cualificado. - *Reglamento eIDAS***
Parte que confía Parte informada*	**Persona física o jurídica que confía en una identificación electrónica o en un servicio de confianza. - *Reglamento eIDAS*** **En el caso de Cartera IDUE, la parte que recibe la información de identificación electrónica o de atributos procedente de Cartera IDUE.**
Divulgación selectiva.*	**Capacidad de la cartera IDUE que permite al usuario presentar un subconjunto de atributos de entre los que figuran en los DIP/PID o en los TE(C)A/(Q)EAA.**
*Confianza**	**La confianza es la característica por la que una parte está dispuesta a confiar en una tercera entidad para que ejecute una serie de acciones y/o realice una serie de afirmaciones sobre una serie de temas y/o ámbitos.[9].**
*Marco de confianza**	**Conjunto jurídicamente exigible de normas y acuerdos operativos y técnicos que rigen un sistema de múltiples intervinientes diseñado para realizar determinados tipos de transacciones entre una comunidad de participantes y sujeto a un conjunto común de requisitos.**

[9] Según especificaciones de "OASIS Trust", [en línea]. Disponible: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html.

Modelo de confianza *	**Conjunto de normas que garantizan la legitimidad de los componentes y las entidades que intervienen en el ecosistema de la Cartera IDUE.**
Proveedor de servicios de confianza (PSC)	*En inglés, Trust Service Provider (TSP)* **Persona física o jurídica que presta uno o varios Servicios de confianza, ya sea como Prestador de Servicios de confianza cualificado o como Prestador de Servicios de confianza no cualificado. - *Reglamento eIDAS***
Servicio de confianza	**Un servicio electrónico prestado normalmente previo pago que consiste en:** **(a) la creación, verificación y validación de certificados electrónicos que respaldan firmas electrónicas y sellos electrónicos, la emisión de sellos de tiempo electrónicos, la prestación de servicios de entrega electrónica certificada y la prestación de servicios de testimonio electrónico de atributos;** **(b) la creación, verificación y validación de certificados para la autenticación de sitios web;** **(c) la conservación de documentos electrónicos que incluyen firmas electrónicas o sellos electrónicos;** **(d) el archivo electrónico de documentos electrónicos;** **(e) la gestión de dispositivos remotos de creación de firmas y sellos electrónicos, bajo control de su titular, securizando el empleo de claves privadas y certificados;** **(f) el registro de datos electrónicos en un libro diario de movimientos semejante a un registro de contabilidad electrónico. - *Propuesta de modificación del Reglamento eIDAS***
*Lista de confianza**	**Repositorio de información sobre entidades dotadas de autoridad en un determinado contexto legal o contractual que proporciona información sobre su estado actual e histórico. Las listas de confianza pueden implementarse de diferentes maneras.**
*Usuario**	**Es una persona física o jurídica que utiliza una Cartera IDUE.**
*Instancia de cartera IDUE**	**Instancia de una Solución de Cartera IDUE perteneciente a un Usuario y que está bajo su control.**
*Proveedores de carteras IDUE**	**Organización, pública o privada, responsable del funcionamiento de una solución de cartera IDUE compatible con eIDAS que puede instanciarse, por ejemplo, mediante su instalación e inicialización.**

Solución Cartera IDUE.*	**Una solución de cartera IDUE es el conjunto de productos y servicios completo propiedad de un proveedor de carteras IDUE, ofrecido a todos los usuarios de dicha solución. Una solución Cartera IDUE puede ser certificada como conforme con IDUE por un CAB.**

Cuadro 1. Definiciones

** Adicional a las definiciones del artículo 3 del Reglamento eIDAS o su propuesta de modificación.*

3. Casos de uso de la cartera EUDI

El desarrollo de las especificaciones de Cartera IDUE (EUDI Wallet) se rige por casos de uso que facilitan la comprensión de la experiencia del usuario a la vez que captan la propuesta de valor y los requisitos empresariales de la Cartera IDUE. Para ello, el Grupo de Expertos de eIDAS comienza creando modelos de servicio para cada caso de uso de la Cartera IDUE. Estos esquemas son representaciones visuales de los distintos componentes y procesos que intervienen en la prestación de un servicio a los usuarios y sirven como herramienta para identificar posibles áreas de mejora, optimizar la experiencia del usuario y agilizar la prestación del servicio. Estos esquemas sirven de base para establecer reglas de uso y especificaciones comunes para todos los casos de uso.

Los esquemas de servicio del caso de uso se encuentran en los anexos como documentos adjuntos. Es importante señalar que los esquemas de servicio ofrecen una solución viable para cada caso de uso, pero existen alternativas y pasos opcionales. Por ejemplo, mostrar datos almacenados para los que el usuario ya ha dado su consentimiento puede ser opcional. Además, los recorridos del usuario (user journeys) pueden variar en función del enfoque de implementación elegido, como el almacenamiento asíncrono de atributos o la recuperación síncrona. Esto podría afectar a aspectos como la prestación del consentimiento para recuperar y compartir datos.

El Grupo de Expertos eIDAS ha descrito esquemas de servicio para los siguientes casos de uso.

3.1 Identificación y autenticación para acceder a los servicios en línea

El objetivo principal de la Cartera IDUE es ofrecer una identificación y autenticación seguras de los usuarios con un alto Nivel de Aseguramiento (Level of Assurance, LoA) para los servicios en línea públicos y privados. Esta funcionalidad esencial garantiza que las Partes Informadas puedan verificar con seguridad que están interactuando con la persona correcta.

En este caso, el usuario utiliza la Cartera IDUE para confirmar su identidad. Accede con frecuencia a servicios en línea que exigen autenticación y actualmente emplea varios métodos para verificar su identidad al acceder a estos servicios. Al usuario también le preocupa compartir datos de identificación personal (PID) durante las interacciones en línea. Sus objetivos incluyen identificarse con servicios que requieren la identificación del usuario y mantener el control sobre el intercambio de datos personales.

Este caso de uso abarca todo el ciclo de vida de la Cartera IDUE desde el punto de vista del usuario, desde la obtención de una Cartera válida hasta la identificación y autenticación del usuario dentro de un servicio en línea. La descripción actual se centra en un flujo remoto viable del mismo dispositivo (véase la sección 6.4), en el que un Usuario persona física emplea un único dispositivo móvil tanto para securizar la sesión como para acceder a la información del servicio.

11

3.2 Permiso de conducción móvil

Un caso de uso significativo para la Cartera IDUE consiste en permitir a los usuarios adquirir, almacenar y mostrar un documento digital como el carné de conducir móvil (movile Driving License, mDL) para demostrar su habilitación para conducir. En este caso, el usuario utiliza la Cartera IDUE para presentar el permiso a un tercero, como un agente de policía.

La descripción del caso de uso se centra en los flujos de proximidad supervisados y no supervisados, que implican escenarios en los que el usuario se encuentra físicamente cerca de una Parte Informada, y el intercambio y divulgación 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 Cartera IDUE presenta los atributos mDL a una Parte Informada humana o bajo su supervisión (con ayuda de un dispositivo); mientras que, en el flujo *no supervisado*, la Cartera IDUE presenta los atributos mDL a una máquina sin supervisión humana.

3.3. Otros casos de uso

En versiones posteriores de este documento, los siguientes casos de uso se detallarán como modelos de servicio:

- *Salud*

El fácil acceso a los datos sanitarios es crucial tanto en contextos nacionales como transfronterizos. La Cartera IDUE puede permitir el acceso a la ficha del paciente, recetas electrónicas, etc.

- *Formación y cualificaciones profesionales*

Facilitar documentos para los procedimientos de convalidación de cualificaciones puede resultar costoso y llevar mucho tiempo a los usuarios finales, empresas y empleadores, proveedores de educación y formación y otras instituciones académicas. Por ejemplo, los testimonios digitales de diplomas se podrían presentar de forma transfronteriza en un formato verificable, fiable y consumible a otra institución educativa o de formación o a un posible empleador. La cartera IDUE permite recoger credenciales digitales educativas

en forma de Testimonios Electrónicos de Atributos facilitando que los alumnos las recopilen y las presenten.

- *Finanzas digitales*

La cartera IDUE facilitará el cumplimiento de los requisitos de autenticación reforzada del cliente en entornos financieros. En consonancia con la Estrategia de Pagos Minoristas de la Comisión[10] el caso de uso se desarrollará en estrecha coordinación con los grupos consultivos de los Estados miembros sobre pagos minoristas y con el sector financiero.

- *Credencial digital de viaje*

La Cartera IDUE puede almacenar credenciales digitales de viaje que permiten a los usuarios beneficiarse de viajes más fluidos.

Este trabajo podrá ampliarse en el futuro a otros casos de uso.

[10] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre una estrategia de pagos minoristas para la UE COM/2020/592 final.

4. Ecosistema europeo de carteras de identidad digital

Este capítulo describe el ecosistema de la Cartera IDUE tal y como está previsto en la propuesta legislativa de la Comisión Europea para la reforma del Reglamento UE 910/2014.

4.1. Funciones en el ecosistema

Las funciones del ecosistema Cartera IDUE se describen en la Figura 1 y se detallan en las secciones siguientes.

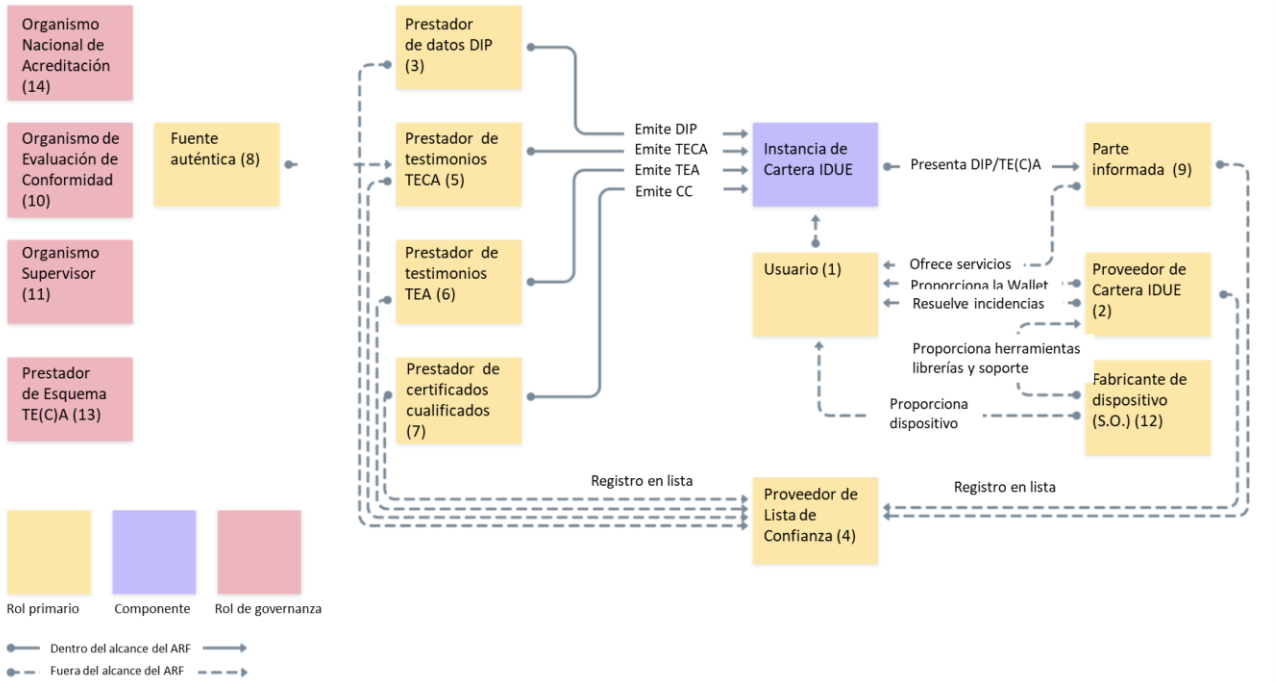


Figura 1: Visión general de las funciones de la cartera IDUE

1. *Usuarios finales de las Carteras IDUE*
2. *Proveedores de Carteras IDUE*
3. *Proveedores de Datos de Identificación de Personas*
4. *Proveedores de Listas de Confianza*
5. *Proveedores de testimonios electrónicos cualificados de atributos (TECA/QEAA)*
6. *Proveedores testimonios electrónicos no cualificados de atributos (TEA/EAA)*
7. *Proveedores cualificado o no cualificados de certificados de firma electrónica/sello electrónico*
8. *Fuentes auténticas*
9. *Partes informadas*
10. *Organismos de Evaluación de la Conformidad (OEC)*
11. *Organismos de supervisión*
12. *Fabricantes de dispositivos y proveedores de subsistemas relacionados*
13. *Proveedores de esquemas de testimonios TEA/EAA o TECA/QEAA*
14. *Organismos nacionales de acreditación*

4.1.1. Usuarios de Cartera IDUE

Los usuarios de Carteras IDUE utilizan la Cartera IDUE para recibir, almacenar y presentar testimonios (DIP/PID, TECA/QEAA o TEA/EAA) sobre sí mismos, incluso para demostrar su identidad. Los usuarios pueden crear Firmas y Sellos Electrónicos Cualificados (QES) utilizando una Cartera IDUE.

En función de la legislación nacional se determina quién puede ser usuario de una cartera IDUE. El uso de una cartera IDUE no es obligatorio para los ciudadanos según la propuesta de revisión del Reglamento EIDAS. Sin embargo, los Estados miembros están obligados a ofrecer al menos una solución de cartera IDUE a sus ciudadanos.

4.1.2. Proveedor de carteras IDUE

Los proveedores de carteras IDUE son Estados miembros u organizaciones autorizadas o reconocidas por los Estados miembros que ponen la cartera IDUE a disposición de los usuarios finales. Corresponde a cada Estado miembro determinar los términos y condiciones del mandato o reconocimiento.

Los Proveedores de Carteras IDUE ponen a disposición de los Usuarios a través de una Solución de Cartera IDUE una combinación de varios productos y Servicios de Confianza previstos en la propuesta de revisión del Reglamento EIDAS, que dan al Usuario el control total sobre el uso de sus Datos de Identificación de Persona (DIP/PID) y Testimonios Electrónicos de Atributos Cualificados o no Cualificados (TECA/QEAA o TEA/EAA), y cualquier otro dato personal dentro de su Cartera IDUE. Desde un punto de vista técnico, esto también puede implicar garantizar al Usuario el control exclusivo sobre el material criptográfico sensible (por ejemplo, claves privadas) relacionado con el uso de estos datos en algunos escenarios, incluida la identificación electrónica, o la realización de firmas o sellos electrónicos.

Los proveedores de carteras IDUE son responsables de garantizar el cumplimiento de los requisitos para las carteras IDUE.

4.1.3. Proveedores de Datos de Identificación de la Persona (DIP/PID)

Los proveedores de DIP/PID son entidades de confianza responsables de:

- verificar la identidad del Usuario de Cartera IDUE de conformidad con los requisitos de Nivel de Aseguramiento Alto (LoA high),
- expedir DIP/PID a la Cartera IDUE en un formato común armonizado y
- facilitar información[11] para que las Partes Informadas verifiquen la validez del DIP/PID.

Corresponde a cada Estado miembro determinar las condiciones de estos servicios.

Los proveedores de DIP/PID pueden ser, por ejemplo, las mismas organizaciones que hoy en día expiden documentos de identidad oficiales, medios de identidad electrónicos,

[11] Sin perjuicio del mecanismo concreto por el que se facilite la información, ya sea directa o indirectamente

proveedores de carteras IDUE, etc. Los proveedores de carteras IDUE pueden ser o no las mismas organizaciones que los proveedores de DIP/PID.

4.1.4. Proveedores de Listas de confianza

El estatus específico de un rol en el ecosistema Cartera IDUE deberá poder ser verificado de forma fidedigna. Tales roles son:

- Proveedores de carteras IDUE
- Proveedores de Datos de Identificación de Personas
- Proveedores de testimonios electrónicos de atributos cualificados (TECA/QEAA)
- Proveedores de Certificados cualificados para firma y sello electrónicos (CC/QC)
- Partes informadas (en ciertas ocasiones, Partes que Confían)
- Proveedores no cualificados de testimonios electrónicos de atributos (TEA/EAA)
- Proveedores de Certificados no cualificados para firma y sello electrónicos
- Proveedores de otros servicios de confianza
- Catálogos de atributos y Esquemas para proveedores de testimonio de atributos

Otras funciones pueden ser necesarias y, por tanto, deben definirse y mencionarse explícitamente en función de la función específica y de su criticidad, por ejemplo, las diferentes funciones y actores implicados en los procesos de firma a distancia.

Cuando se utiliza, una Lista de Confianza[12] debe contar con un mecanismo que permita incorporar o retirar información sobre las entidades fiables del ámbito concreto al que se refiere manteniendo el registro de tales entidades y proporcionando a terceros su información. Corresponde a cada entidad gestora de una lista de confianza (registrador) establecer las condiciones que deben cumplir las entidades para figurar en la lista, al menos que vengan predeterminadas por una normativa ya existente, por ejemplo, en normativa sectoriales.

4.1.5. Proveedores de Testimonio electrónico cualificado de atributos

Los testimonios TEA/EAA cualificados las prestan los PCSC (Prestadores Cualificados de Servicios de Confianza, en inglés QTSP, Qualified Trust Service Providers). El marco de confianza general para los PCSC se aplica también a los TECA/QEAA, pero también es necesario definir normas específicas para este servicio de confianza. Los proveedores de TECA/QEAA mantienen una interfaz para solicitar y proporcionar TECA/QEAA, incluida una interfaz de autenticación mutua con las carteras IDUE y, potencialmente, una interfaz hacia fuentes auténticas para verificar atributos. Los Proveedores de TECA/QEAA proporcionan información o la ubicación de los servicios que se pueden

[12] Más adelante se aportarán más precisiones sobre cómo podrían aplicarse las listas de confianza.

utilizar para preguntar sobre el estado de validez de los TECA/QEAA, sin poder recibir ninguna información sobre el uso de los testimonios. Corresponde a cada PCSC determinar los términos y condiciones de estos servicios, más allá de lo especificado en el Reglamento eIDAS.

4.1.6. Proveedores de Testimonio electrónico no cualificado de atributos

Los TEA no cualificados los pueden proporcionar proveedores de servicios de confianza cualificados o no cualificados. Aunque están supervisados según el marco regulatorio de eIDAS, cabe suponer que otros marcos jurídicos o contractuales distintos del eIDAS rigen en su mayoría las normas de prestación, uso y reconocimiento de los TEA ya existentes.

Estos otros marcos pueden abarcar áreas de política como los permisos de conducir, credenciales educativas o pagos digitales, aunque también pueden recurrir a proveedores cualificados de testimonio electrónico de atributos. Para que se utilicen los TEA, los PSC/TSP ofrecen a los usuarios una forma de solicitar y obtener TEA, lo que significa que deben cumplir técnicamente las especificaciones de la interfaz de Cartera IDUE. Dependiendo de las reglas del dominio, los proveedores de TEA/EAA pueden proporcionar información sobre la validez de los TEA/EAA, sin tener la posibilidad de recibir ninguna información sobre el uso que la Parte Informada hará de los TEA/EAA. Las condiciones de emisión de los TEA y los servicios conexos están sujetos a normas sectoriales.

Los prestadores cualificados y no cualificados de DIP/PID, TEA/EAA y TECA/QEAA también pueden recibir la denominación de **Partes Informantes**, por contraste con las *partes que confían* en los testimonios que reciben y se denominan también **Partes Informadas**.

4.1.7. Prestadores de Certificados Cualificados y No Cualificados para Firma y sellos electrónicos

El apartado 3 del artículo 6 bis del texto denominado “COM(2021)281 final” que contiene la propuesta de modificación del Reglamento EIDAS exige que la cartera IDUE permita al usuario crear firmas o sellos electrónicos cualificados. Este objetivo puede alcanzarse de varias maneras:

- La cartera IDUE está certificada como dispositivo cualificado de creación de firma o sello (DCCF o DCCS, en inglés Qualified Signature/Seal Creation Device, QSCD), o bien
- Implementa capacidades seguras de autenticación e invocación para la realización de firma/sello como parte de un DCCF/QSCD local o un DCCF/QSCD remoto gestionado por un PCSC/QTSP.

Las interfaces de Cartera IDUE con los DCCF/QSCD se ampliarán en futuras versiones de este documento ARF.

4.1.8. Proveedores de otros servicios de confianza

La interacción de Cartera IDUE con proveedores de otros servicios de confianza cualificados o no cualificados, como los sellos de tiempo, podrá describirse con más detalle en futuras versiones de este documento ARF.

4.1.9. Fuentes auténticas

Las Fuentes Auténticas son los repositorios o sistemas públicos o privados reconocidos o exigidos por la ley que contienen atributos sobre una persona física o jurídica. Las fuentes auténticas en el ámbito del anexo VI de la propuesta de revisión del Reglamento EIDAS son fuentes de atributos sobre dirección, edad, sexo, estado civil, composición familiar, nacionalidad, títulos y licencias de educación y formación, títulos y licencias de cualificaciones profesionales, permisos y licencias públicos, datos financieros y empresariales. Las Fuentes Auténticas incluidas en el ámbito de aplicación del Anexo VI deben proporcionar interfaces a los Proveedores de TECA/QEAA para verificar la autenticidad de los atributos mencionados, ya sea directamente o a través de intermediarios designados reconocidos a nivel nacional. Las fuentes auténticas también pueden emitir testimonios TE(C)A/(Q)EAA por sí mismas si cumplen los requisitos del Reglamento eIDAS. Corresponde a los Estados miembros definir los términos y condiciones para la prestación de estos servicios, pero de acuerdo con las especificaciones técnicas, normas y procedimientos mínimos aplicables a los procedimientos de verificación de los testimonios electrónicos cualificadas de atributos.

4.1.10. Partes Informadas (o Partes que confían)

Las Partes Informadas son personas físicas o jurídicas que confían en una identificación electrónica o en un servicio de confianza. En el contexto de las carteras IDUE, solicitan los atributos necesarios contenidos en el conjunto de datos DIP/PID, TECA/QEAA y TEA/EAA de los usuarios de carteras IDUE para confiar en la cartera IDUE, previa aceptación por parte del propietario de la cartera (usuario) y dentro de los límites de la legislación y las normas aplicables. La razón para confiar en la cartera IDUE puede ser un requisito legal, un acuerdo contractual o la propia decisión de la entidad informada. Para recibir información de una Cartera IDUE, las Partes Informadas deben notificar al Estado Miembro en el que están establecidas sobre su intención de recibir información procedente de Carteras IDUE. Las Partes que confían deben mantener una interfaz con Cartera IDUE para solicitar testimonios con autenticación mutua. Las partes Informadas son responsables de autenticar los DIP/PID y los TE(C)A/(Q)EAA.

4.1.11. Organismos de evaluación de la conformidad (OEC)

Las carteras IDUE deben estar certificadas por organismos públicos o privados acreditados designados por los Estados miembros[13]. Los PCSC deben ser auditados periódicamente por organismos de evaluación de la conformidad (OEC, en inglés, CAB, Conformity Assessment Bodies). Los OEC/CAB están acreditados por un organismo nacional de acreditación de conformidad con el Reglamento 765/2008 como responsables de llevar a cabo las evaluaciones en las que los Estados miembros tendrán que basarse antes de expedir una Cartera IDUE o proporcionar el estatus de "cualificado" a un Proveedor de Servicios de Confianza. Las normas y regímenes utilizados por los OEC/CAB para desempeñar sus tareas de evaluación/homologación de las carteras IDUE se especifican más adelante en el proceso "Toolbox".

4.1.12. Organismos de supervisión

Los Estados miembros deben notificar a la Comisión Europea la designación de organismos de supervisión cuya misión es supervisar a los PCSC/QTSP y actúan, en caso necesario, en relación con los proveedores de servicios de confianza no cualificados.

4.1.13. Fabricantes de dispositivos y entidades relacionadas

Las carteras IDUE dispondrán de varias interfaces con los dispositivos en los que se basen, que podrán tener las siguientes finalidades:

- Almacenamiento local.
- Acceso a Internet en línea.
- Sensores como cámaras de smartphone, sensores infrarrojos, micrófonos, etc.
- Canales de comunicación offline como Bluetooth Low Energy (BLE), tecnología "WIFI Aware", Near Field Communication (NFC).
- Emisores como pantallas, linternas, altavoces, etc.
- Tarjetas inteligentes y elementos seguros (SE, componente de smartphone).

Para el almacenamiento seguro de material criptográfico, se puede establecer una interfaz con dispositivos o servicios específicos. Otras entidades relacionadas pueden ser proveedores de servicios, como proveedores de servicios en la nube, proveedores de tiendas de aplicaciones App, etc.

La propuesta legal de reforma del reglamento EIDAS establece restricciones (por ejemplo, el cumplimiento de Nivel de Aseguramiento Alto – "LoA high") respecto a qué tipos de dispositivos y servicios se pueden utilizar con el fin de emitir el Cartera IDUE. Del mismo modo, la disponibilidad, así como los términos y condiciones de los proveedores de interfaces

[13] Artículo 6 quater, apartado 3

de dispositivos y proveedores de servicios relacionados, establecerán otras restricciones para los proveedores de carteras IDUE.

4.1.14. Proveedores de esquemas de Testimonios Electrónicos de atributos Cualificado y No cualificados

Los proveedores de esquemas TE(C)A/(Q)EAA publican esquemas y vocabularios que describen la estructura y la semántica de los testimonios TE(C)A/(Q)EAA. Lo que puede permitir a otras entidades, como las partes informadas, el descubrimiento y validación de los TE(C)A/(Q)EAA. La Comisión Europea establece las especificaciones técnicas, normas y procedimientos mínimos a tal efecto. La existencia de esquemas comunes, incluso por parte de organizaciones sectoriales específicas, es fundamental para la adopción generalizada de los TE(C)A/(Q)EAA.

4.1.15. Organismos nacionales de acreditación

Los Organismos Nacionales de Acreditación (ONA, en inglés NAB, National Accreditation Bodies) con arreglo al Reglamento (CE) nº 765/2008[14] son los organismos de los Estados miembros que realizan la acreditación con autoridad derivada del Estado miembro. Los ONA/NAB acreditan a los OEC/CAB como organismos de certificación profesional competentes, independientes y supervisados encargados de certificar productos/servicios/procesos haciendo uso de documento(s) normativo(s) que establecen los requisitos (por ejemplo, legislaciones, especificaciones, perfiles de protección, normas técnicas). Los ONA/NAB supervisan los OEC/CAB a los que han expedido un certificado de acreditación.

4.2. Ciclo de vida de una cartera IDUE

El texto de propuesta de reforma del Reglamento EIDAS define la cartera IDUE con un alto nivel de abstracción, así como a los proveedores de carteras IDUE que tienen la obligación legal de garantizar que los habitantes/residentes de un Estado miembro puedan obtener una cartera IDUE válido y plenamente funcional. El ciclo de vida de una Cartera IDUE tendrá algunas interacciones con los Proveedores de Listas de Confianza que especifican el estado de un rol en el ecosistema de Carteras IDUE de una manera fiable. Desarrollar una Arquitectura y un Marco de Referencia que deben servir de guía para el desarrollo de dicho Cartera IDUE requiere un nivel de abstracción más detallado para ser eficiente y producir una descripción de la arquitectura lo suficientemente expresiva como para ser prescriptiva.

[14] Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93.

Este capítulo parte de un modelo de objetos mínimo y define el ciclo de vida de los conceptos centrales: Solución de Cartera IDUE, DIP/PID, TE(C)A/(Q)EAA e Instancia de Cartera IDUE. Esos conceptos se han elegido como punto de partida porque el desarrollo conjunto del ARF mostró que los ciclos de vida de estos conceptos están estrechamente entrelazados, lo que llevó a una descripción poco clara y, en consecuencia, provocó malentendidos.

El modelo de objetos se ampliará según sea necesario en futuras versiones del ARF.

4.2.1. Modelo simplificado de cartera IDUE

En la Figura 2 se distinguen los conceptos de Solución de Cartera IDUE e Instancia de Cartera IDUE. Una Solución Cartera IDUE es el producto y/o servicio completo proporcionado por un Proveedor de Cartera IDUE. Una Instancia de Cartera IDUE es una instancia personal de una Solución Cartera IDUE que se ejecuta en un dispositivo del usuario al que pertenece y que es quien la controla.

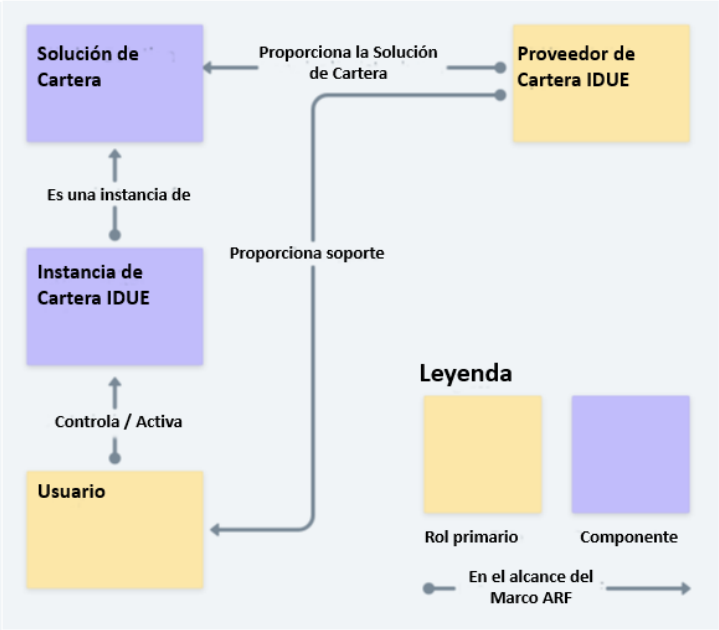


Figura 2: Modelo simplificado de objetos de cartera IDUE

Esta definición no es prescriptiva del factor de forma, por lo que, dependiendo de la implementación, una Instancia de Cartera IDUE puede consistir en una única aplicación móvil, o en un conjunto de componentes locales y remotos disponibles para un Usuario específico.

4.2.2. Ciclos de vida de los DIP/PID y de los TE(C)A/(Q)EAA

Los ciclos de vida de los DIP/PID y de los TE(C)A/(Q)EAA son esencialmente idénticos, sin embargo, para el alcance de esta descripción nos referiremos posteriormente sólo a la EPI. El texto de esta sección aplicado a la EPI se aplica mutatis mutandis a los TE(C)A/(Q)EAA.

El DIP/PID en el contexto de la Cartera IDUE comienza su ciclo de vida cuando se emite a una Instancia de Cartera IDUE. Tenga en cuenta que esto significa que la gestión de atributos en la fuente auténtica (respetando las estructuras nacionales y las definiciones de atributos) queda fuera del ámbito del ARF.

Hay que tener en cuenta que, para determinados casos de uso, los DIP/PID pueden estar preaprovisionados, lo que significa que aún no son válidos cuando se emiten, pero alcanzan su validez más tarde. Si los DIP/PID se emiten en la fecha de inicio de validez o después, se considera inmediatamente que el estado cambia directamente a válido si la fecha de comprobación es posterior a la de inicio de validez. Esto significa que los DIP/PID podrían estar "preemitidos".

Figura 3: Diagrama de estados del DIP/PID

Existen dos transiciones posibles de un DIP/PID válido: o bien expira automáticamente, por superarse la *"fecha de fin de validez*", o bien es revocado activamente por su Proveedor antes de su expiración. La expiración y la revocación son transiciones esencialmente independientes. Una vez que el DIP/PID ha caducado o se ha revocado, no puede volver a ser válido. La actualización del DIP/PID (por ejemplo, debido a un cambio de nombre) siempre requiere una nueva emisión.

4.2.3. Ciclo de vida de la solución Cartera IDUE

Una Solución Cartera IDUE tiene un estado propio, tal y como se define en el artículo 10 bis del futuro Reglamento. El estado de la Solución afecta al estado de todas las Instancias de Cartera IDUE de dicha Solución de Cartera IDUE. El estado "**Candidato"** es el primer estado

de una Solución Cartera IDUE. Esto significa que está totalmente implementada y que el Proveedor de Carteras IDUE solicita que la solución se certifique como Cartera IDUE.

Si se han cumplido todos los criterios legales y técnicos, incluida la certificación de la Solución Cartera/Wallet por el OEC/CAB, entonces un Estado miembro puede decidir empezar a proporcionar **Instancias** de la Solución a los Usuarios. El estado de la Solución pasa a ser "**válido**". De conformidad con el artículo 6 quinquies, el Estado miembro informará a la Comisión de cualquier cambio en el estado de certificación de su Solución Cartera/Wallet. Esto significa que la solución Cartera IDUE se puede lanzar **oficialmente** y que se pueden proporcionar instancias de la solución a los usuarios.

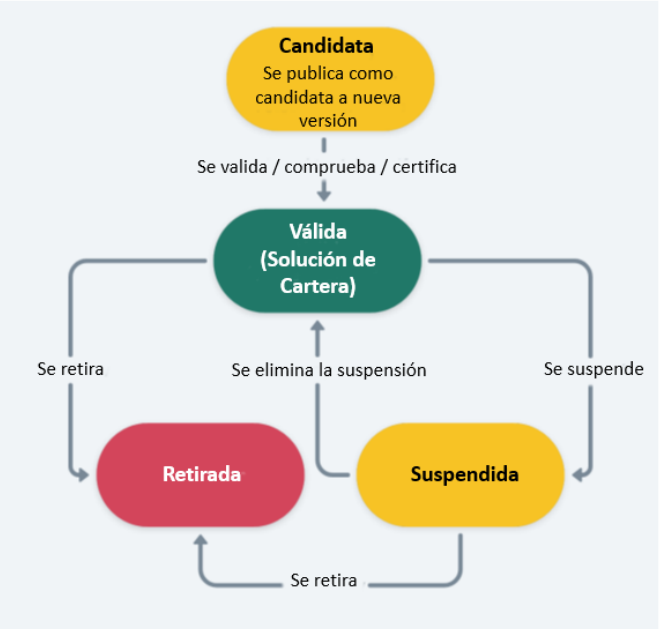


Figura 4: Diagrama de estado de la solución Cartera/Wallet

En las condiciones legales del artículo 10 bis, apartado 1, el Estado miembro emisor puede suspender temporalmente una Solución Cartera IDUE. Esto podría ser, por ejemplo, como consecuencia de un problema crítico de seguridad en esa Solución Cartera IDUE. Esto da lugar al estado de "**suspendida**". De conformidad con el apartado 2 del artículo 10 bis, el Estado miembro emisor puede cancelar la suspensión de la Solución Cartera/Wallet y continuar con la emisión, devolviendo la Solución al estado "**válido**". De conformidad con el apartado 3, la solución Cartera IDUE puede retirarse y cancelarse por completo.

4.2.4. Ciclo de vida de la instancia de cartera IDUE

Una Instancia de Cartera IDUE comienza su vida basándose en una Solución de Cartera IDUE válida. El Proveedor de Cartera IDUE proporciona una Solución de Cartera IDUE al Usuario que se considera que ejecuta una Instancia de Cartera en estado "**operativo**" una vez instalada y activada por el Usuario en su dispositivo. Dependiendo del factor de forma y de la implementación, proporcionar una instancia puede requerir varias acciones, por ejemplo,

instalación e inicialización en el caso de una Cartera IDUE móvil. Una Instancia de Cartera IDUE de este tipo podría utilizarse ya para funciones no específicas de IDUE, como almacenar tarjetas de fidelidad o billetes de tren no personalizados o cualquier otro certificado que no exija la vinculación a unos DIP/PID válidos.

Una vez que se inicializa una Instancia de Cartera IDUE, se considera "**válida**", lo que significa que es reconocida por un Proveedor de DIP/PID y que posee un conjunto de DIP/PID válidos. Si los DIP/PID caducan o se revocan, la Cartera IDUE no queda automáticamente inutilizada, sino que su estado rebajado a "**operativo**". Esto puede afectar a la validez de un testimonio TE(C)A/(Q)EAA o de un certificado cualificado para firma o sellos electrónicos.

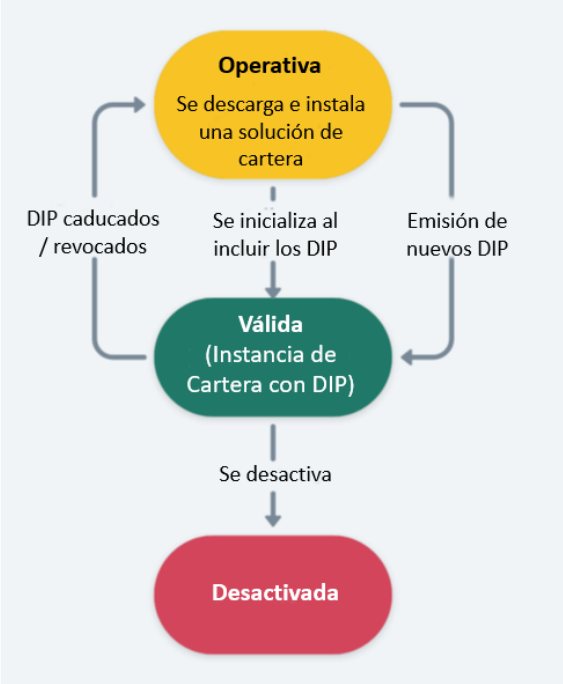


Figura 5: Diagrama de estado de la instancia de cartera

Actualmente se asume que sólo el Usuario[15] podrá desactivar una Instancia de Cartera IDUE. Hay que tener en cuenta que esto es independiente de la posibilidad de que un prestador de datos DIP/PID o un proveedor de testimonio TE(C)A/(Q)EAA revoquen sus testimonios.

[15] Por ejemplo, en caso de fallecimiento del usuario o de vulnerabilidad de la seguridad de Cartera IDUE.

5. Requisitos para la expedición de DIP/PID y TE(C)A/(Q)EAA

5.1. Datos de identificación de la persona

En este capítulo se detalla el conjunto DIP/PID presentado por la Cartera IDUE.

Un proveedor de DIP/PID puede emitir un conjunto de datos DIP/PID para la cartera IDUE y permitir el uso de la cartera IDUE como medio de identificación electrónica al acceder a servicios en línea y fuera de línea.

Los mecanismos a través de los cuales se genera el DIP/PID y se proporciona a la Cartera IDUE dependen de los Estados miembros y sólo están limitados por requisitos legales como los requisitos de nivel de aseguramiento (LoA High), RGPD/GDPR o cualquier otra ley nacional o de la Unión Europea.

A continuación se describirá el formato de los datos tal y como se presentan a la Parte usuaria, sin hacer ninguna suposición sobre cómo la cartera IDUE recuperó o generó estos datos de antemano.

5.1.1 El conjunto de datos

5.1.2.1. Principios para la revisión del conjunto DIP/PID

Este capítulo propone una revisión de los conjuntos de datos opcionales eIDAS especificados en la norma derivada de eIDAS "CIR 2015/1501"[16] y se analizan otras especificaciones, la minimización de datos y los identificadores.

La revisión del conjunto de datos opcionales eIDAS que aquí se propone se construye sobre la base de los siguientes principios:

- No debe haber dos personas con el mismo conjunto de atributos obligatorios DIP/PID.
- El conjunto de DIP/PID debe contener al menos el conjunto mínimo de atributos especificados en el Reglamento de Ejecución "CIR 2015/1501" como obligatorios.

[16] Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, relativo al marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- El conjunto de datos obligatorios se limita por naturaleza a la intersección (estrecha) de lo que todos los Estados miembros pueden proporcionar para todas las personas físicas y jurídicas y lo que se necesita a efectos de identificación electrónica.

5.1.1.1. Atributos del DIP/PID para personas físicas

La siguiente tabla ofrece una visión general de los atributos DIP/PID incluidos actualmente en el marco eIDAS, así como de los atributos opcionales adicionales que se sugiere incluir.

Atributos eIDAS obligatorios	Atributos eIDAS opcionales	Posibles atributos opcionales adicionales
Apellido(s) actual	**Apellido(s) de nacimiento**	**Nacionalidad/Ciudadanía***
Nombres actuales	**Nombres de nacimiento**	
Fecha de nacimiento	**Lugar de nacimiento**	**Atributos opcionales utilizados a nivel nacional, por ejemplo, número de identificación fiscal, número de la seguridad social, etc.**
Identificador único	**Dirección actual**	
	Género	

Cuadro 2 - Atributos obligatorios y opcionales del los DIP/PID para las personas físicas

**Nacionalidad/Ciudadanía - se trata de un posible atributo multivalor porque los ciudadanos pueden tener más de una nacionalidad. Sin embargo, la nacionalidad/ciudadanía también puede comunicarse en forma de TE(C)A/(Q)EAA, para permitir a los ciudadanos demostrar una nacionalidad determinada, sin actualizar el conjunto de DIP/PID ni implicar al proveedor de DIP/PID.*

Se han añadido posibles atributos opcionales adicionales para facilitar una gama más amplia de opciones de autenticación tanto en línea como fuera de línea, así como para abordar el aprendizaje derivado de las actuales implementaciones de eIDAS.

Los metadatos asociados a los DIP/PID pueden detallar adicionalmente la fecha de emisión y/o caducidad, la autoridad emisora y/o el Estado miembro, la información necesaria para realizar la vinculación del titular y/o la prueba de posesión, la información o localización de los servicios que pueden utilizarse para consultar el estado de validez de los atributos y potencialmente más información.

5.1.2 Requisitos de expedición del EPI

En el cuadro siguiente se definen los requisitos aplicables a los DIP/PID en relación con la información que se incluye en el certificado, por ejemplo, a efectos de comprobación de validez, autenticidad, validación, políticas, modelo de datos y formatos.

Las futuras versiones de este texto podrán ampliar la tabla para especificar requisitos. Hay que tener en cuenta que estos requisitos están dirigidos principalmente a la primera versión de las especificaciones de la solución Cartera IDUE, y que pueden cambiar a medida que evolucionen las especificaciones.

#	Requisito
1	**El testimonio sobre DIP/PID DEBE contener la información necesaria para identificar al proveedor de DIP/PID.**
2	**El testimonio sobre DIP/PID DEBE contener la información necesaria para realizar una comprobación de la integridad de los datos.**
3	**El testimonio sobre DIP/PID DEBE contener la información necesaria para verificar su autenticidad.**
4	**El testimonio sobre DIP/PID DEBE contener toda la información necesaria para realizar comprobaciones del estado de validez del testimonio.**
5	**El testimonio sobre DIP/PID DEBE incluir toda la información (como atributo o como cualquier otro valor firmado) necesaria para realizar la verificación de la vinculación del titular por una Parte Informada.**
6	**El testimonio sobre DIP/PID DEBE emitirse para ser presentada de acuerdo tanto con el modelo de datos especificado en la norma ISO/IEC 18013-5:2021 como con el Modelo de datos de credenciales verificables v1.1 del W3C.**
7	**El testimonio sobre DIP/PID DEBE codificarse como CBOR y en formato JSON.**
8	**El testimonio sobre DIP/PID DEBE permitir la divulgación selectiva de atributos mediante el uso del esquema "Selective Disclosure for JWTs (SD-JWT)" y "Mobile Security Object (ISO/IEC 18013-5)" de acuerdo con el modelo de datos (Permiso de conducir en el móvil).**
9	**El testimonio sobre DIP/PID DEBE utilizar firmas electrónicas y formatos de cifrado tal y como se detalla en la RFC 8812 Concise Binary Object Representation (CBOR) Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms.**
10	**El testimonio sobre DIP/PID DEBE utilizar algoritmos de firma y cifrado de conformidad con la norma SOG-IS ACM (Agreed Cryptographic Mechanism)[17].**

Cuadro 3 - Requisitos de expedición de EPI

[17] https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

5.2. Testimonio electrónico de atributo cualificado y no cualificado

5.2.1 Requisitos de expedición de los TE(C)A/(Q)EAA

En el cuadro siguiente se definen los requisitos aplicables a los Testimonios TE(C)A/(Q)EAA en relación con la información que se incluye en el Testimonio, por ejemplo, a efectos de comprobación de validez, autenticidad, validación, políticas relacionadas con la gestión de claves, el modelo de datos y los formatos.

Los testimonios TE(C)A/(Q)EAA también pueden emitirse con arreglo a los requisitos aplicables a los Datos DIP/PID.

Las futuras versiones de este texto podrán ampliar la tabla para especificar requisitos. Hay que tener en cuenta que estos requisitos están dirigidos principalmente a la primera versión de las especificaciones de la solución Cartera IDUE, y que pueden cambiar a medida que evolucionen las especificaciones.

#	Requisito
1	**Los testimonios TE(C)A/(Q)EAA DEBEN contener la información necesaria para identificar al Emisor.**
2	**Los testimonios TE(C)A/(Q)EAA DEBE Ncontener la información necesaria para realizar una comprobación de la integridad de los datos.**
3	**Los testimonios TE(C)A/(Q)EAA DEBEN contener la información necesaria para verificar su autenticidad.**
4	**Los testimonios TE(C)A/(Q)EAA DEBEN contener toda la información necesaria para realizar comprobaciones de su estado de validez.**
5	**(no se indica)**
6	**Los testimonios TE(C)A/(Q)EAA DEBERÍAN incluir toda la información (como atributo o como cualquier otro valor firmado) necesaria para realizar la verificación de la vinculación del titular por parte de una Parte Informada.**
7	**Los testimonios TE(C)A/(Q)EAA DEBEN expedirse de conformidad con una de las especificaciones del modelo de datos: la norma de codificación de permiso de conducir: I"SO/IEC 18013-5:2021", o "Verifiable Credentials Data Model v1.1" (Modelo de datos de credenciales verificables 1.1) del W3C.**

8	**Los testimonios TE(C)A/(Q)EAA DEBERÍAN codificarse como uno de los siguientes formatos: CBOR o JSON según el modelo de datos utilizado para la certificación. Ver RFC 8812, RFC 8152, RFC 9052, RFC 9053**
9	**Los testimonios TE(C)A/(Q)EAA PUEDEN codificarse como JSON-LD (JSON for Linking Data).**
10	**Los testimonios TE(C)A/(Q)EAA DEBERÍAN permitir la Revelación Selectiva de atributos utilizando bien "Selective Disclosure for JWTs" (Revelación Selectiva para JWTs) (SD-JWT) o bien el esquema "Mobile Security Object" (Objeto de Seguridad Móvil) de la norma sobre permiso de conducir (ISO/IEC 18013-5) de acuerdo con el modelo de datos utilizado para el testimonio.**
11	**Los testimonios TE(C)A/(Q)EAA DEBERÍAN utilizar uno de los siguientes formatos de firma y cifrado según se detalla en las normas del IETF, RFC relativas a JOSE (Javascript Object Signing and Encryptio), y RFCs relativas a COSE (CBOR Object Signing and Encryption) RFCs de acuerdo con el modelo de datos utilizado para el testimonio.**
12	**Los testimonios TE(C)A/(Q)EAA DEBERÍAN utilizar algoritmos de cifrado de conformidad con la norma SOG-IS ACM (Agreed Cryptographic Mechanism)**
13	**Los testimonios TE(C)A/(Q)EAA DEBERÍAN emitirse de acuerdo con el protocolo OpenID4VCI (OpenID for Verifiable Credential Issuance).**

Cuadro 4 - Requisitos de expedición de las (Q)CEA

6. Arquitectura de referencia y flujos

La arquitectura de referencia representa un conjunto de decisiones tomadas durante el proceso de diseño de la arquitectura de las soluciones de Cartera IDUE. Estas elecciones se basaron en la necesidad de que las soluciones de Cartera IDUE soporten varios escenarios en los que el usuario, la parte que confía (o parte informada), o ambos, estén fuera de línea, al tiempo que proporcionan flexibilidad a los Estados miembros para implementar una solución de Cartera IDUE en varias configuraciones de componentes.

6.1. Consideraciones sobre el diseño

Para limitar la complejidad, las especificaciones iniciales de la Solución de Cartera IDUE incluirán sólo un número mínimo de componentes de la solución que permitan el uso de la Instancia de Cartera IDUE para la identificación del Usuario, de forma que pueda funcionar como un medio de Identidad Electrónica (eID).

Las opciones elegidas no reflejan una importancia relativa ni un compromiso a largo plazo. En su lugar, la selección se ha guiado por factores como la disponibilidad y madurez de las normas y especificaciones, una estimación de la facilidad de adopción y el grado de flexibilidad (en términos de casos de uso permitidos) que ofrece cada componente de la solución.

Los componentes de la solución aquí propuestos evidencian la expectativa actual de utilizar la serie de normas ISO/IEC 23220, una vez disponibles públicamente, para futuras versiones del ARF (Cards and security devices for personal identification — Building blocks for identity management via mobile devices).

6.2. Componentes de arquitectura

Los siguientes componentes han sido identificados como los bloques de construcción de la arquitectura de la cartera IDUE necesarios para implementar una Solución de Cartera IDUE:

- **Sistema de gestión de claves criptográficas.** Este componente se encarga de gestionar y almacenar información criptográfica como las claves privadas generadas, por ejemplo, durante el proceso de emisión de DIP/PID.

- **Protocolo de intercambio de testimonios**. Este protocolo define cómo solicitar y presentar los datos DIP/PID y los testimonios TE(C)A/(Q)EAA de forma segura y preservando la privacidad. El protocolo también define cómo se realiza la autenticación entre la Parte que Confía (o Parte Informada) y la Instancia de Cartera IDUE, en particular el mecanismo a través del cual la Parte Informada puede solicitar la identificación a través de la Cartera IDUE. La solicitud contiene toda la información necesaria sobre la Parte Informada y los datos solicitados. Este protocolo se ocupa de la negociación de la confianza y la autenticación mutua.

- **Protocolo de emisión**. El protocolo define cómo deben expedirse los DIP/PID y los testimonios TE(C)A/(Q)EAA y en qué formatos.

- **Modelo de datos**. El modelo de datos define y describe los elementos de datos y cómo interactúan entre sí y sus propiedades.

- **Esquemas DIP/PID y TE(C)A/(Q)EAA**. El esquema de testimonio contiene la estructura y la organización lógica de los datos que definen las propiedades del testimonio, los atributos del Usuario. El esquema de testimonio también contiene información adicional que incluye, entre otras cosas, los mecanismos de verificación, la garantía de identidad subyacente (nivel de aseguramiento) y el marco de confianza con el que se relacionan las propiedades, así como la prueba de posesión por parte del usuario legítimo.

- **Formatos de DIP/PID y TE(C)A/(Q)EAA**. Los formatos de DIP/PID y TE(C)A/(Q)EAA se utilizan para representar la característica, cualidad, derecho o permiso de una persona física o jurídica o de un objeto, en forma de artefactos digitales firmados electrónicamente y verificables, que contienen cualquier propiedad adicional a efectos de interoperabilidad.

- **Formatos de firma**. Implementación técnica de uno o varios métodos matemáticos en forma de artefacto digital, destinada a demostrar la autenticidad de un documento digital, su integridad, autenticar al autor de un documento y, opcionalmente, también a su destinatario (audiencia del documento).

- **Modelo de confianza.** Conjunto de normas que garantizan la legitimidad de los componentes y las entidades que intervienen en la infraestructura de Cartera IDUE, y que abarcan:
  - Autenticación de usuarios.
  - Identificación del emisor.
  - Registro de emisores.
  - Modelos de datos y esquemas reconocidos.
  - Registro y autenticación de las partes Informadas.
  - Mecanismos para establecer la confianza en un escenario multidominio.

  Los componentes del modelo de confianza permiten identificar a las entidades que confían en Cartera IDUE y son fundamentales para la autenticidad, confidencialidad, integridad y el consentimiento informado (en las firmas electrónicas y sellos) de la información. Existen diferentes modelos de confianza basados en distintas normas.

La lista de confianza es un mecanismo en el marco de un modelo de confianza para publicar y obtener información sobre partes que ostentan autoridad, por ejemplo, emisores de DIP/PID, de testimonios TE(C)A/(Q)EAA y partes informadas.

- **Suites y mecanismos criptográficos**. Algoritmos y métodos que aseguran el intercambio de datos en términos de confidencialidad e integridad.

- **Identificadores de entidad**. Identificadores únicos para todos los elementos del modelo de datos.

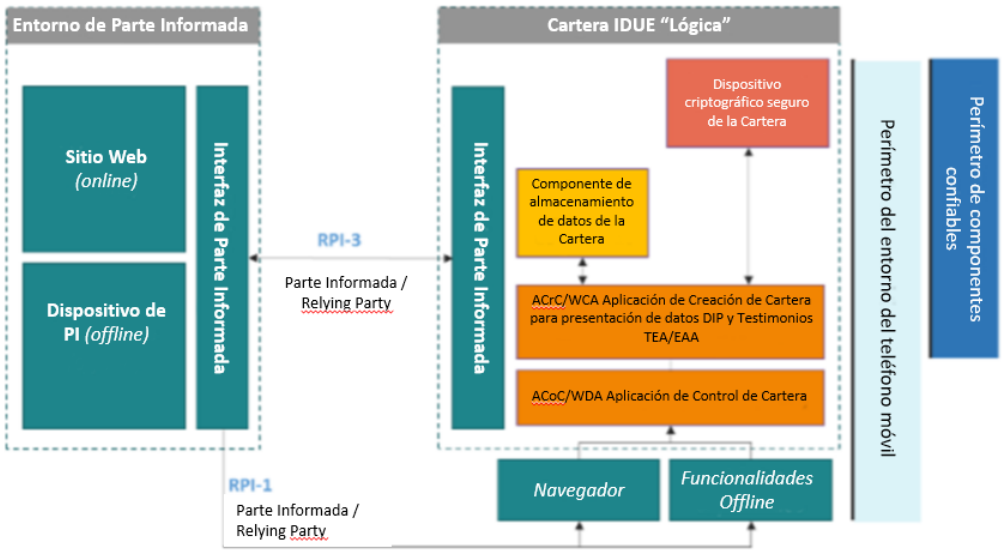
- **Comprobación del estado de validez**. Mecanismo para publicar y obtener información sobre el estado de validez de, entre otros, de datos DIP/PID, de testimonios TE(C)A/(Q)EAA, certificados destinados a realizar firmas o sellos electrónicos, etc.

6.3. Arquitectura lógica

Cuando una solución de Cartera IDUE tiene una aplicación que se ejecuta en un dispositivo móvil, puede existir la necesidad de componentes de confianza adicionales que no forman parte de esa aplicación pero que, sin embargo, forman parte de los recursos lógicos de la Cartera IDUE. Esta necesidad puede surgir por varias razones:

- Seguridad: por ejemplo, si un dispositivo concreto no dispone de hardware suficientemente seguro, como un “Secure Element” (elemento seguro, equipamiento estándar de muchos móviles), pueden ser necesarios componentes de hardware externos, como tarjetas inteligentes.
- Reutilización de sistemas en entornos de servidor remoto (backend).
- Reutilización de la infraestructura de identidad centrada en el usuario (denominada a veces identidad descentralizada).

Estos componentes de confianza pueden ser: almacenamiento externo de confianza, hardware externo o integrado de confianza u otros componentes remotos de Cartera IDUEs. A continuación, se muestra una representación conceptual de las variaciones en la implementación de los componentes de Cartera IDUE:



ACrA/WCA: Crea la presentación (verificable) de DIP y Testimonios Cualificados que se comparten con la Parte informada, según la información recibida de la ACoC/WDA.

ACoC/WDA: Proporciona los datos elegidos por el usuario:

- DIP y testimonios (que se pueden combinar)
- Determina cuales se pueden (o no) presentar

Figura 6: Modelo conceptual de las configuraciones de Cartera IDUE

La tabla siguiente relaciona los componentes de la cartera IDUE con el modelo conceptual de la figura 6.

Bloque funcional en el modelo conceptual	Componentes aplicables a la solución de Cartera IDUE
Dispositivo criptográfico seguro de la Cartera IDUE	Claves de usuario y certificados
	Entorno seguro y aislado para claves y datos
	Algoritmos criptográficos (por ejemplo, simétricos, asimétricos, derivación de claves, funciones hash, generación de números aleatorios) y protocolos (por ejemplo, ECDH, TLS).
	Entorno seguro definido por hardwqre para claves y datos: un Elemento Seguro (SE), Entornos de Ejecución de Confianza (Trusted Execution Environment -TEEs), Módulo de Seguridad de Hardware (Hardware Security Module - HSM), etc. (remoto o local).
	Datos de autenticación (PIN, biometría)
Componentes de almacenamiento de datos de la cartera IDUE	Identificador único y persistente del usuario
	Atributos del usuario
	Datos personales y atributos del usuario
	Entorno seguro para claves y datos

Cartera IDUE "Presentación de DIP/PID o TEA/EAA" Aplicación de creación de Cartera (WCA - Wallet Creation Application)	Registros, historial de operaciones de la Instancia de Cartera IDUE, telemetría
	Identificador de la Instancia de aplicación Cartera IDUE (por ejemplo, configuración, fabricante y versión)
	Interfaces internas de la instancia de Cartera IDUE (por ejemplo, entre almacenamiento, componentes, cifrado)
Aplicación de control de Cartera IDUE (WDA, Wallet Driving Application)	Registros, historial de operaciones de la Instancia de Cartera IDUE, telemetría
	Identificador de la aplicación de Instancia de Cartera IDUE (por ejemplo, configuración, fabricante y versión)
	Interfaz de usuario de la Cartera IDUE
Interfaz de la parte informada	Interfaz de la Cartera IDUE con (Q)TSP, con proveedores de TE(C)A/(Q)EAA, infraestructuras de los Estados miembros, e-ID nacionales, partes que confían y otras fuentes de EEA.
	Canales de comunicación (en línea/fuera de línea) entre la cartera IDUE y otras partes

Tabla 5 - Correspondencia entre los componentes de la cartera IDUE y los bloques funcionales del modelo conceptual

La tabla siguiente asigna los componentes de la Cartera IDUE a los dos perímetros representados en la Figura 6.

Perímetros	**Componentes aplicables a la solución Cartera IDUE**
Perímetros de los posibles componentes de confianza	Información sobre el dispositivo (tipo, configuración, versión de firmware, estado, etc.)
	Claves y certificados del sistema
	Sistemas back-end (servidores de bases de datos)
	Dispositivos conectados de confianza
Perímetro móvil potencial	Información sobre el dispositivo (tipo, configuración, versión de firmware, estado, etc.)
	Sensores del smartphone: cámara, lector NFC, sensor de huellas dactilares, acelerómetro, etc.

Cuadro 6: correspondencia entre los componentes de la cartera IDUE y los perímetros

6.4. Tipos de flujos

Esta sección describe los cuatro tipos de flujos que Cartera IDUE DEBE soportar a nivel general. Los cuatro flujos son los siguientes:

1. Flujo supervisado de proximidad.
2. Flujo de proximidad no supervisado.
3. Flujo remoto entre dispositivos.
4. Flujo remoto del mismo dispositivo.

Los flujos 1 y 2 están relacionados con un escenario en el que el usuario de Cartera IDUE se encuentra físicamente cerca de una parte que confía (parte informada) y el intercambio y la divulgación de testimonios (DIP/PID y/o TECA/QEAA) deben producirse utilizando protocolos de proximidad (NFC, Bluetooth, QR-Code, etc.), sin que el usuario tenga conectividad a Internet (nótese que esto no implica que sea posible cualquier otra función aparte del transporte sin conexión). Los dos flujos de proximidad difieren en un aspecto importante. En el flujo supervisado, la Cartera IDUE presenta atributos verificables a, o bajo la supervisión de, una persona que actúa como parte informada (que puede operar un dispositivo propio). En el flujo no supervisado, la Cartera IDUE presenta atributos verificables a una máquina sin supervisión humana.

Los flujos 3 y 4 están relacionados con un escenario en el que el intercambio de datos debe producirse a través de Internet. Los dos flujos remotos difieren en un aspecto importante. En el flujo remoto entre dispositivos, el usuario de la Cartera IDUE consume información del servicio en un dispositivo distinto del dispositivo de la Cartera IDUE, que sólo se utiliza para asegurar la sesión (por ejemplo, utilizando Cartera IDUE para escanear un código QR en una página de inicio de sesión para acceder a una cuenta bancaria en su navegador web). En cambio, en el flujo remoto del mismo dispositivo, el usuario de Cartera IDUE utiliza el dispositivo de la Cartera IDUE tanto para asegurar la sesión como para consumir la información del servicio.

Las experiencias de los usuarios se basarán en al menos uno de los cuatro flujos descritos, y probablemente en una combinación de ellos. Obsérvese que los cuatro flujos pueden implementarse de múltiples maneras. Las implementaciones específicas quedan fuera del ámbito de este texto.

Es necesario seguir estudiando los dos flujos de proximidad, ya que son posibles con o sin conexión a Internet. Entre los posibles escenarios figuran:

- el Usuario y la Parte Informada están ambos en línea,
- sólo el Usuario está conectado,

- sólo la Parte Informada está en línea,
- El usuario y la Parte Informada están desconectados.

Para todos los flujos descritos anteriormente y, en concreto, para el flujo no supervisado de proximidad, la autorización del usuario es un requisito previo para el intercambio de datos.

A continuación, se detallan las configuraciones iniciales del DIP/PID y del TEA/EAA (en el futuro podrán añadirse configuraciones según sea necesario).

6.5. Configuraciones de la cartera

6.5.1. Justificación

Uno de los objetivos del desarrollo de la Cartera IDUE es armonizar los datos DIP/PID y los testimonios TE(C)A/(Q)EAA a través de las fronteras. Idealmente, esto implica un número muy reducido de soluciones técnicas diferentes para limitar la complejidad, lo que facilita la implantación y adopción. Por otro lado, la especificación de Cartera IDUE debe dar soporte a una amplia gama de casos de uso con diferentes requisitos. Estas diferencias motivan formas específicas de crear, solicitar y presentar datos DIP/PID y testimonios TE(C)A/(Q)EAA. Para satisfacer estas necesidades, las soluciones de Cartera IDUE implementarán configuraciones. Una configuración es un conjunto específico de restricciones y formas de utilizar las capacidades técnicas de la Solución de Cartera IDUE para gestionar tanto el conjunto de DIP/PID como los testimonios TE(C)A/(Q)EAA.

El primer propósito de una configuración es vincular las capacidades específicas de la Cartera IDUE con los requisitos de los casos de uso que se pueden cumplir con estas capacidades. Una sola configuración debe soportar múltiples casos de uso; cada uno conforme a la configuración específica para la cual se emitió el DIP/PID o el testimonio TE(C)A/(Q)EAA.

El segundo y último propósito de una configuración es proporcionar una herramienta para ampliar potencialmente los entornos tecnológicos y las características de las especificaciones de la Solución de Cartera IDUE. Si un caso de uso, o un grupo de casos de uso, no puede basarse en una configuración existente de la Solución de Cartera IDUE, se introduce la necesidad de incluir una configuración adicional para dar soporte a los requisitos que no pueden satisfacerse con las configuraciones existentes. En el capítulo 8 se describen la gobernanza y el proceso para añadir nuevas configuraciones.

6.5.2. Configuraciones iniciales

Las Soluciones de Cartera IDUE admitirán inicialmente dos configuraciones:

- La configuración de **tipo 1** está dirigida específicamente a los casos de uso en los que la parte Informada confía en las garantías requeridas para el nivel de aseguramiento alto de la identidad (LoA High), tal como se define en el Reglamento de Ejecución CIR 2015/1502[18] para permitir la identificación transfronteriza utilizando atributos DIP/PID en nivel de aseguramiento de la identidad (LoA High). La configuración de Tipo 1 está diseñada principalmente para fines de establecimiento de datos de identidad DIP/PID.

[18] Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, por el que se establecen especificaciones técnicas mínimas y procedimientos relativos a los niveles de garantía de los medios de identificación electrónica de conformidad con el artículo 8, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- La configuración de **Tipo 2** tiene como objetivo permitir flexibilidad y soporte de características adicionales para posibles casos de uso de testimonios TE(C)A/(Q)EAA que no puedan ser satisfechos por la configuración de Tipo 1 (por ejemplo, posiblemente en áreas de salud, credenciales de educación, ...).

Hay que tener en cuenta que la configuración de Tipo 1 no está pensada únicamente para el conjunto de DIP/PID. Es probable que muchos testimonios TE(C)A/(Q)EAA se utilicen en ámbitos que requieran niveles de aseguramiento altos (por ejemplo, finanzas, sanidad, acceso a edificios) y tengan requisitos que se satisfagan con la configuración de Tipo 1. De ser así, estos TE(C)A/(Q)EAA se expedirán con arreglo a la configuración de Tipo 1.

6.5.3. Requisitos de configuración

Esta sección establece los requisitos de las configuraciones comparando la configuración de Tipo 1 y Tipo 2 en diferentes grupos de requisitos. Las futuras versiones de este texto podrán ampliar la tabla para especificar los requisitos relativos, por ejemplo, a los Emisores y a las Partes que Confían. Hay que tener en cuenta que estos requisitos están dirigidos principalmente a la primera versión de las especificaciones de la Solución de Cartera IDUE, y que pueden cambiar a medida que evolucionen las especificaciones.

La siguiente tabla define los requisitos aplicables a los componentes de la Solución de Cartera IDUE para soportar las dos configuraciones. Según el tipo de configuración el requisito implica sustituir los puntos suspensivos [...] por el verbo indicado en la columna Tipo 1 o Tipo 2 (DEBE, DEBERÍA, etc).

Componente	**Requisito**	**Tipo 1**	**Tipo 2**
Sistema de gestión de claves criptográficas - 1	La Solución de Cartera IDUE [...] basarse en uno de los siguientes componentes para almacenar y gestionar claves criptográficas: Elemento seguro (SE) integrado o entorno de (para dispositivos móviles), dependencia de un dispositivo externo (elementos seguros / tarjetas inteligentes), y un servidor (módulo de seguridad de hardware remoto). La elección del hardware seguro que se utilizará y soportará depende de cada solución de Cartera IDUE.	DEBE	DEBERÍA

Sistema de gestión de claves criptográficas - 2	La Solución de Cartera IDUE [...] aplicar medidas de seguridad para evitar la exportación de secretos criptográficos.	DEBE	DEBERÍA
Protocolo de intercambio de testimonios - 1	La Solución de Cartera IDUE [...] soportar OpenID4VP como protocolo de intercambio de testimonios para **flujos remotos.** Cuando se solicita autenticación pseudónima, los parámetros de solicitud DEBERÍAN especificarse de acuerdo con la especificación OpenID SIOPv2.	DEBE	PUEDE
Protocolo de intercambio de testimonios - 2	La Solución de Cartera IDUE [...] soportar el protocolo detallado en la norma ISO/IEC 18013-5:2021 para **flujos de proximidad**.	DEBE	PUEDE
Protocolo de intercambio de testimonios - 3	La Solución de Cartera IDUE [...] realizar comprobaciones para hacer cumplir la vinculación de sesión (es decir, solicitud de atributo para DIP/PID).	DEBERÍA	PUEDE
Protocolo de intercambio de testimonios - 4	La Solución de Cartera IDUE [...] soportar alternativas de protocolo de intercambio de testimonios[19].	PUEDE	PUEDE
Protocolo de intercambio de testimonios - 5	La Solución de Cartera IDUE [...] poder realizar una prueba de posesión.	DEBE	PUEDE
Protocolo de intercambio de testimonios - 6	La Solución de Cartera IDUE [...] soportar la Divulgación Selectiva de atributos tal y como se especifica en la norma ISO/IEC 18013-5:2021.	DEBE	PUEDE
Protocolo de intercambio de testimonios - 7	La Solución de Cartera IDUE [...] soportar la Divulgación Selectiva de atributos como se especifica en la especificación SD-JWT.	DEBE	PUEDE

[19] Cabe destacar la API REST de mdoc, tal y como se detalla en el borrador e lanorma ISO/IEC 23220-4.

Protocolo de emisión - 1**	La Solución de Cartera IDUE [...] admitir OpenID4VCI como protocolo de emisión. Los Estados miembros son libres de incluir alternativas adicionales al protocolo de emisión en sus soluciones nacionales.	DEBE **	DEBE
Modelo de datos -1	La Solución de Cartera IDUE [...] admitir testimonios emitidos de conformidad con el modelo de datos especificado en la norma ISO/IEC 18013-5:2021.	DEBE	DEBERÍA
Modelo de datos -2	La Solución de Cartera IDUE [...] soportar testimonios emitidos de acuerdo con el modelo de datos especificado en la especificación W3C Verifiable Credentials Data Model 1.1.	DEBE	DEBERÍA
Formatos DIP/PID y TE(C)A/(Q)EAA - 1	La Solución de Cartera IDUE [...] soportar testimonios en formato JWT y SD-JWT.	DEBE	PUEDE
Formatos DIP/PID y TE(C)A/(Q)EAA - 2	La Solución de Cartera IDUE [...] admitir testimonios en formato CBOR.	DEBE	PUEDE
Formatos DIP/PID y TE(C)A/(Q)EAA - 3	La Solución de Cartera IDUE [...] soportar testimonios en formato JSON-LD.	PUEDE	PUEDE
Formatos de firma -1	La Solución de Cartera IDUE [...] soportar formatos de firma electrónica y cifrado de acuerdo con las especificaciones JOSE (JWT).	DEBE	PUEDE
Formatos de firma - 2	La Solución de Cartera IDUE [...] soportar formatos de firma y cifrado de acuerdo con las especificaciones COSE.	DEBE	PUEDE
Formatos de firma - 3	La Solución de Cartera IDUE [...] admitir formatos de firma y cifrado de acuerdo con las especificaciones LD-Proof.	NO DEBE	PUEDE

Suites y mecanismos criptográficos - 1	La Solución de Cartera IDUE [...] soportar suites criptográficas y mecanismos utilizados para atributos detallados en SOG-IS Agreed Cryptographic Mechanisms Version 1.2.	DEBE	DEBERÍA

Tabla 7 - Requisitos de configuración

***Sólo para testimonios TE(C)A/(Q)EAA que deben tener un protocolo de emisión común para garantizar la interoperabilidad. En el caso de los datos DIP/PID, corresponde al Estado miembro definir el protocolo de emisión y cada solución de cartera soportará el protocolo de emisión de DIP/PID específico de acuerdo con las especificaciones del Estado miembro.*

Las soluciones de Cartera IDUE **DEBEN** soportar la configuración de **Tipo 1** que es obligatoria para el DIP/PID.

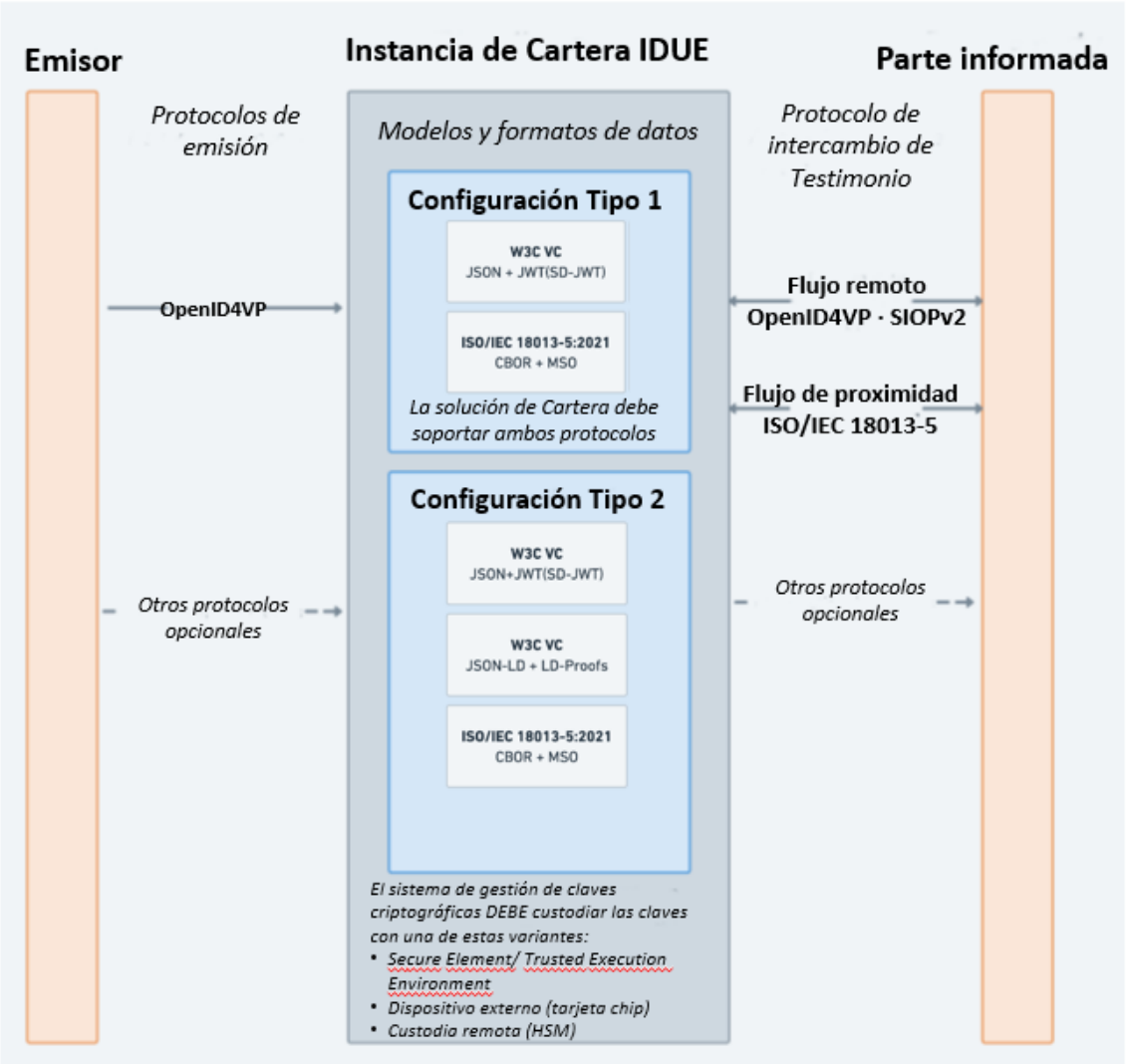


Figura 7. Configuraciones Cartera IDUE.

7. El proceso de certificación de las carteras IDUE

Los Estados miembros, de conformidad con el artículo 6 quater (3) de la propuesta de reforma del Reglamento EIDAS, deben designar a los organismos de evaluación de la conformidad acreditados que supervisarán la realización de la evaluación de la conformidad de las carteras IDUE. Este proceso de designación debe armonizarse entre los Estados miembros.

Una vez efectuada esta designación, los Estados miembros comunicarán a la Comisión Europea los nombres y direcciones de estos organismos públicos o privados con arreglo al apartado 5 del artículo 6 quater de dicha propuesta.

El proveedor de la cartera IDUE debe solicitar (seleccionar, contratar) a uno o varios OEC/CAB designados que evalúen y certifiquen la conformidad de su cartera IDUE con los requisitos del Reglamento eIDAS.

La certificación de la Cartera IDUE la lleva a cabo el OEC/CAB para evaluar y certificar la conformidad de la Cartera IDUE (objetivo de la certificación) con los documentos normativos que se deriven de los actos de ejecución establecidos en el Art. 6a(11) sobre especificaciones técnicas y operativas y normas de referencia.

La Cartera IDUE deberá estar certificada para garantizar las evaluaciones de conformidad, pero también para demostrar el cumplimiento de altos niveles de seguridad. El uso de un sistema de certificación de la ciberseguridad debería aportar un nivel armonizado de confianza en la seguridad de la Cartera IDUE. Se espera que el almacenamiento seguro de material criptográfico también esté sujeto a la certificación de ciberseguridad.

El proceso de certificación de los proveedores de carteras IDUE debe aprovechar, basarse y exigir el uso de los sistemas de certificación pertinentes y existentes del Reglamento sobre la Ciberseguridad,[20] o partes de los mismos, para certificar la conformidad de las carteras, o partes de los mismos, con los requisitos de ciberseguridad aplicables.

[20] REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»)

8. Proceso de desarrollo de la Arquitectura y del Marco de referencia

8.1. Publicación

Este documento y los elementos pendientes se ponen a disposición del público en la dirección electrónica https://code.europa.eu/eudi/architecture-and-reference-framework, donde se actualizará periódicamente según el flujo de trabajo descrito en el capítulo 8.2.

8.2. Actualización

Para garantizar un progreso constante y rápido en la elaboración y actualización de este documento, se aplica el siguiente proceso y metodología de trabajo.

El Grupo de Expertos eIDAS (E03032)[21] deberá mantener un backlog, que es una lista priorizada de elementos de trabajo para completar el ARF. La lista de tareas pendientes se actualizará en función de los comentarios del Grupo de Expertos eIDAS, los Proyectos Piloto a Gran Escala impulsados desde la Agencia HaDEA (DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID[22]), la Comisión u otras partes interesadas, como las organizaciones internacionales de normalización. Por ejemplo, los resultados del desarrollo de la implementación de referencia de la Cartera IDUE (Framework Contract for Fixed Price and Quoted Time and Means for Development, Consultancy and Support for the European Digital Identity Wallet[23]) y los consiguientes borradores de especificaciones técnicas detalladas pueden dar lugar a nuevos elementos de trabajo.

La Comisión Europea (DG CONNECT) organizará el trabajo sobre los temas atrasados y facilitará que el trabajo avance según el calendario previsto.

El Grupo de Expertos de eIDAS debatirá y comparará periódicamente diferentes propuestas relativas a soluciones técnicas, recomendaciones y requisitos relacionados con cada cuestión pendiente pertinente con vistas a actualizar el ARF. A este respecto, el Grupo de Expertos eIDAS mantendrá una lista de Registros de Decisiones de Arquitectura (RDA, en inglés ADR, Architecture Decission Records), de modo que sea posible realizar un seguimiento y comprender la motivación que subyace a las decisiones técnicas descritas en el ARF.

Cualquier cambio y/o actualización de este documento deberá ser acordado por el Grupo de Expertos eIDAS. El Grupo de Expertos eIDAS se reunirá periódicamente con el objetivo de

[21] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3032
[22] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-deploy-02-electronic-id

[23] https://etendering.ted.europa.eu/cft/cft-display.html?cftId=10237

debatir y aprobar nuevas versiones de este documento, así como de actualizar los trabajos pendientes de desarrollo.

Este documento se adaptará al resultado de las negociaciones legislativas de la propuesta de Marco Europeo de Identidad Digital y se actualizará en consecuencia.

8.2.1. Versiones de documentos

Para evitar problemas de interoperabilidad y que los cambios en el ARF pasen desapercibidos, se utilizará para el ARF un sistema de control de versiones y el siguiente esquema semántico de versiones.

El documento ARF tendrá un número de versión determinado siguiendo el formato *MAYOR.MENOR.PARCHE*, donde:

La versión **MAYOR** se incrementa (es decir, hay una nueva versión), cuando el documento ARF ha sufrido cambios significativos, por ejemplo, introduciendo algunos cambios radicales en la arquitectura,

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

La versión **PARCHE** se incrementa cuando se han realizado cambios menores (por ejemplo, corrección de erratas).

9. Referencias

[Palabras clave en el ARF para indicar los niveles de exigencia] https://www.rfc- editor.org/rfc/rfc2119

[ISO/IEC 18013-5] https://www.iso.org/standard/69084.html

[ISO/IEC AWI TS 23220-4] https://www.iso.org/standard/79126.html

[W3C-VC-DATA-MODEL] Sporny, M., Noble, G., Longley, D., Burnett, D. C., Zundel, B. y D. Chadwick, "Verifiable Credentials Data Model 1.0", 19 de noviembre de 2019, <https://www.w3.org/TR/vc-data-model>.

[OpenID4VP] Terbu, O., Lodderstedt, T., Yasuda, K., Lemmon, A., y T. Looker, "OpenID for Verifiable Presentations", 30 de diciembre de 2022, https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[OpenID4VCI] Lodderstedt, T., Yasuda, K., y T. Looker, "OpenID for Verifiable Credential Issuance", 30 de diciembre de 2022, https://openid.net/specs/openid-4verifiable- credential-issuance.html

[SIOPv2] K. Yasuda, T. Lodderstedt, M. Jones, "Self-Issued OpenID Provider V2", 1 de enero de 2023, https://openid.net/specs/openid-connect-self-issued-v2-1_0.html.

[SD-JWT] https://www.ietf.org/archive/id/draft-ietf-oauth-selective-disclosure-jwt-02.html

[W3C StatusList2021] https://w3c-ccg.github.io/vc-status-list-2021/

[COSE] RFC9052 https://www.rfc-editor.org/rfc/rfc9052,
RFC9053 https://www.rfc-editor.org/rfc/rfc9053

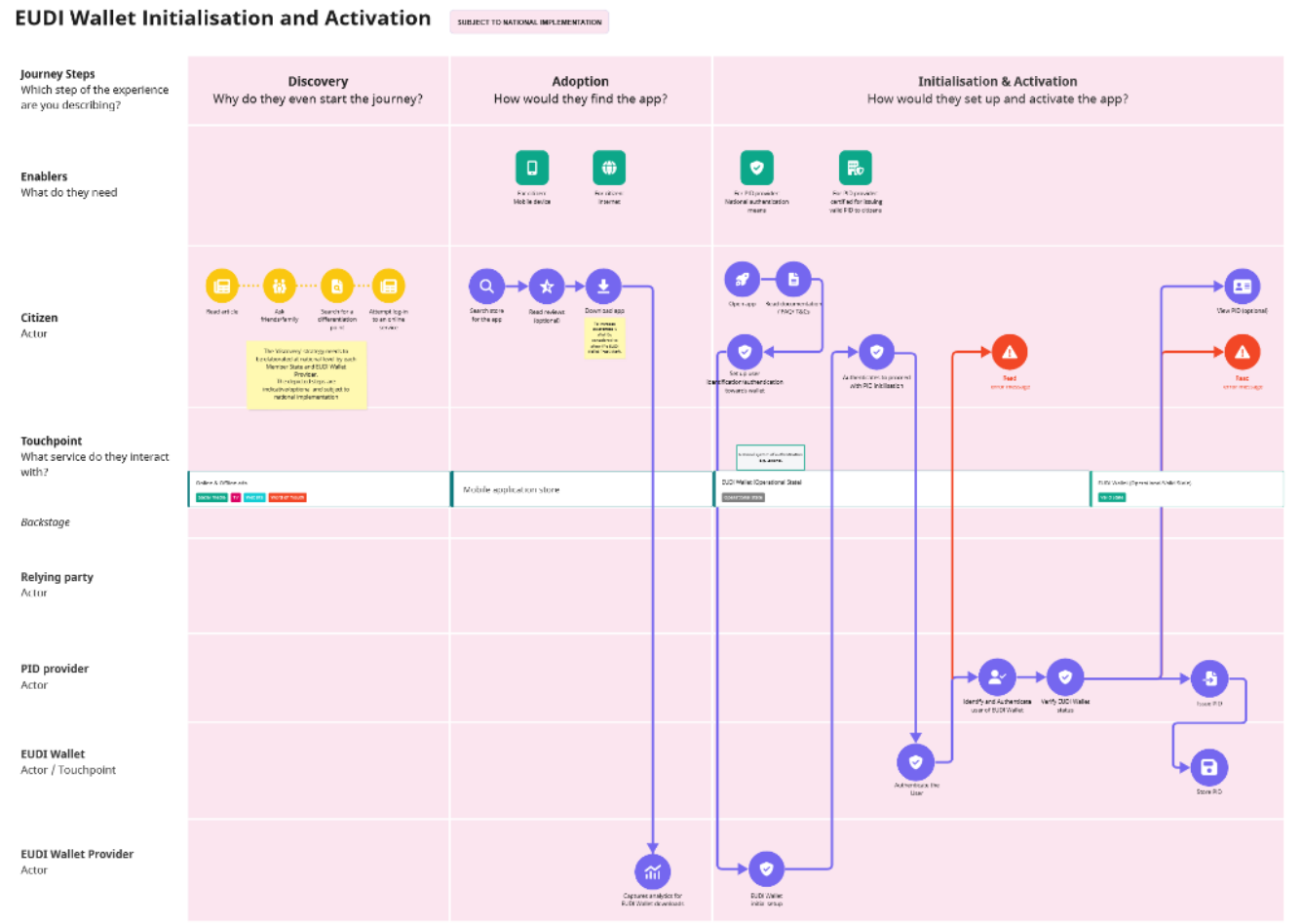
[JOSE] RFC7515 https://www.rfc-editor.org/rfc/rfc7515.html,
RFC7516 https://www.rfc-editor.org/rfc/rfc7516.html,
RFC7517 https://www.rfc-editor.org/rfc/rfc7517.html,
RFC7518 https://www.rfc-editor.org/rfc/rfc7518.html

[SOG-IS] Mecanismos criptográficos acordados v1.2
https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

[JSON-LD] JSON-LD 1.1 Manu Sporny, Dave Longley, Gregg Kellogg, Markus Lanthaler, Pierre-Antoine Champin, Niklas Lindström, https://www.w3.org/TR/json-ld/

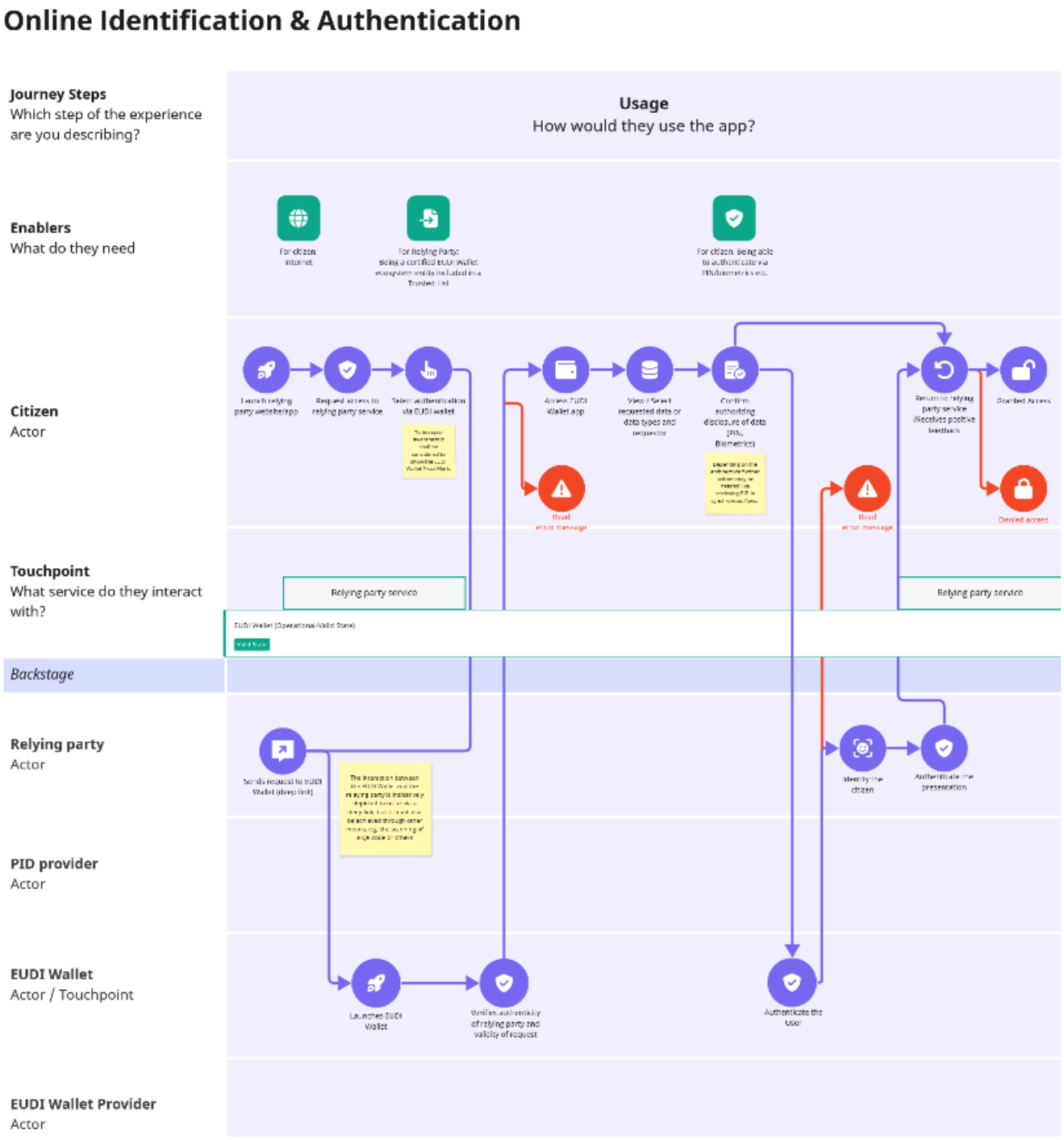
Anexo 01 - inicialización y activación

El modelo de servicio sobre la inicialización y activación de la Cartera se describe en el archivo adjunto ***Anexo 01- EUDI Wallet - Initialisation and Activation.pdf***



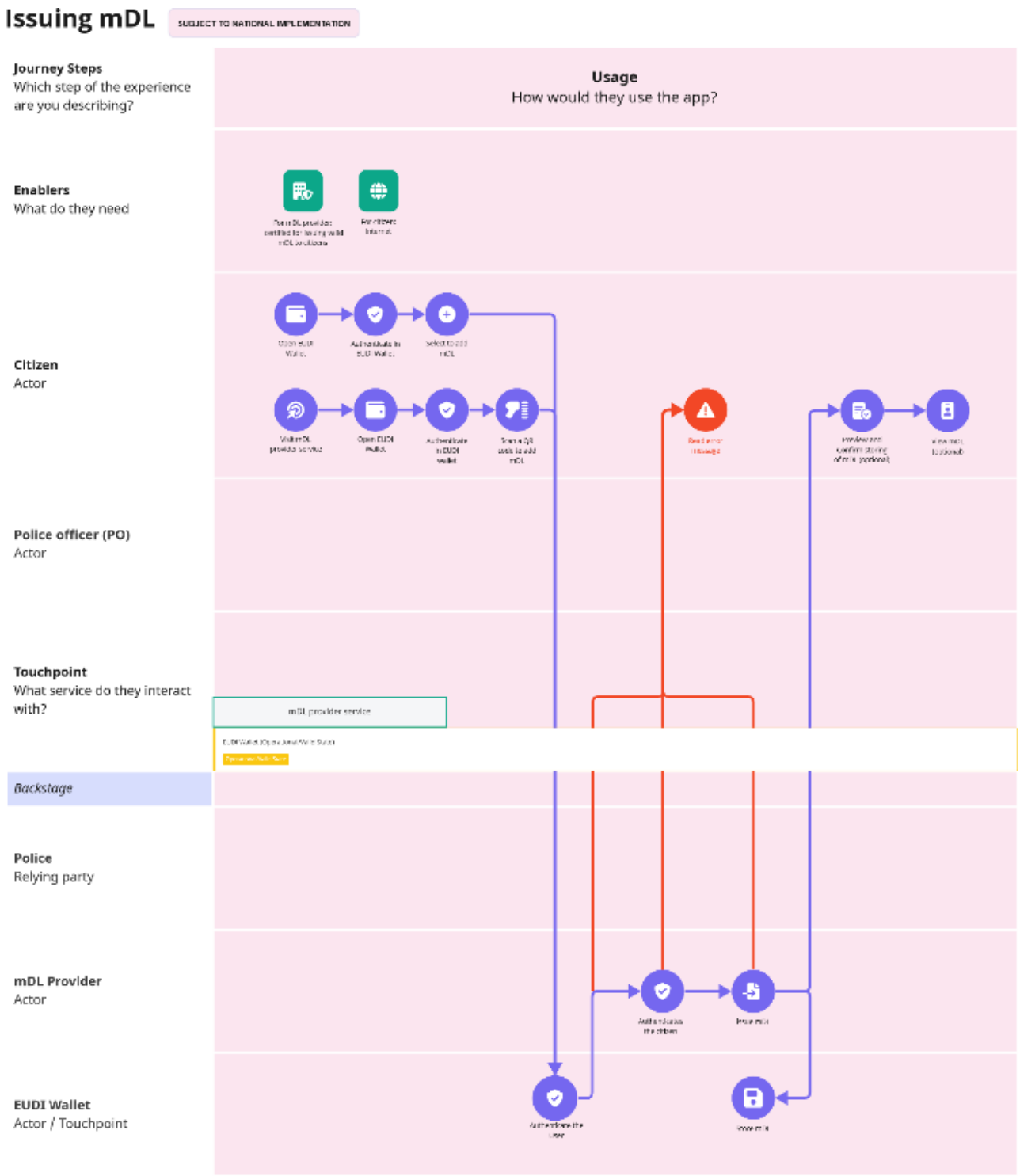
Anexo 02 - identificación y autenticación en línea

El modelo de servicio sobre identificación y autenticación en línea para la Cartera se describe en el archivo adjunto ***Anexo 02- EUDI Wallet - Online Identification and Authentication.pdf***



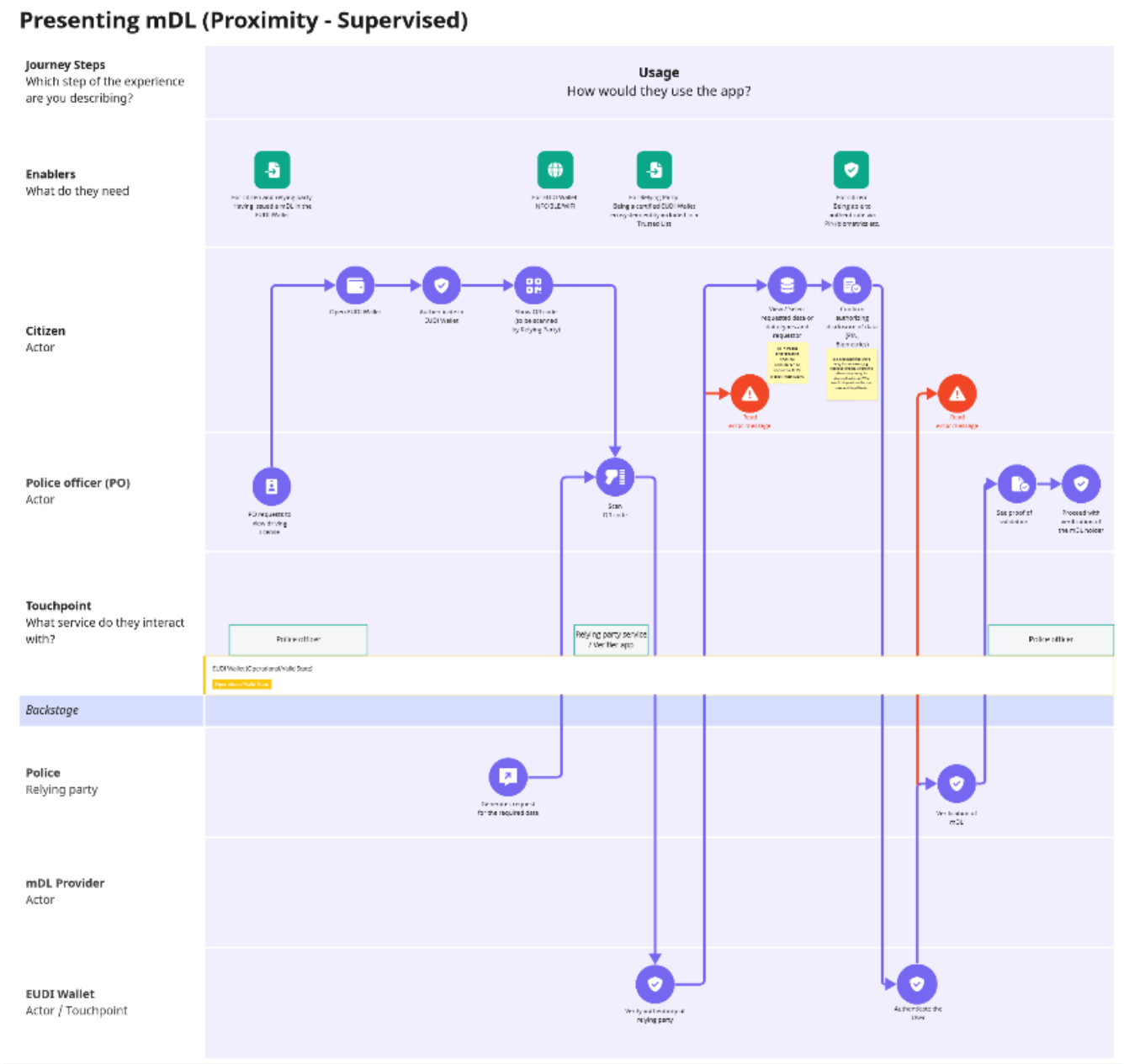
Anexo 03 - Expedición de mDL

El proyecto de servicio sobre la emisión de mDL se describe en el archivo adjunto ***Anexo 03 - EUDI Wallet - issuing mDL.pdf***.



Anexo 04 - presentación de mDL (proximitysupervised)

El proyecto de servicio sobre la presentación ***de mDL (proximidad supervisada)*** se describe en el archivo adjunto ***Anexo 04 - EUDI Wallet - presenting mDL (proximity-supervised).pdf***.



Anexo 05 - presentación de mDL (proximityunsupervised)

El proyecto de servicio sobre la presentación ***de mDL (proximidad-sin supervisión***) se describe en el archivo adjunto ***Anexo 05 - EUDI Wallet - presenting mDL (proximity-unsupervised).pdf***.