Identidad digital europea

Arquitectura y Marco de Referencia

– Esquema –

1 TABLA DE CONTENIDOS

1 INTRODUCCIÓN

Nota sobre la traducción.

La traducción al español del documento "European Digital Identity Architecture and Reference Framework – Outline" (abreviadamente ARF) la ha realizado Julián Inza (julian@inza.com), en el contexto de la Formación impartida por TCAB (Trust Conformity Assessment Body) en 2022 y en la que ha sido uno de los profesores. La Formación de TCAB permite obtener la certificación profesional de Auditor EIDAS.

La traducción del texto y de las ilustraciones se ha realizado en octubre/noviembre de 2022, con pequeñas licencias para que se entiendan mejor algunas expresiones y siglas en inglés, manteniendo en algunos casos las siglas en inglés junto con las correspondientes traducciones en español.

En la fecha en la que se ha completado la traducción se esperaba una versión actualizada (anunciada para el 30 de octubre de 2022) que no ha estado disponible.

Las menciones al artículo 6a, 6b, 6c, … del texto de la Propuesta de modificación del Reglamento EIDAS podrían transformarse en la versión en español en 6 bis, 6 ter, 6 quater,…

El documento original en inglés, de febrero de 2022, está disponible en

- "European Digital Identity Architecture and Reference Framework – Outline" https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

Este documento se denomina "Arquitectura y Marco de Referencia de la Identidad Digital Europea – Esquema –", (abreviadamente AMR).

1.1 CONTEXTO

El 3 de junio de 2021, la Comisión adoptó una Recomendación en la que se pedía a los Estados miembros que trabajaran en el desarrollo de una caja de herramientas que incluyera una arquitectura técnica y un marco de referencia (Architecture and Reference Framework, ARF), un conjunto de normas y especificaciones técnicas comunes y un conjunto de directrices comunes y mejores prácticas. [1]

La Recomendación especifica que estos resultados servirán de base para la aplicación del Reglamento marco europeo de identidad digital una vez adoptado, sin que el proceso de desarrollo de la Caja de Herramientas interfiera o prejuzgue el proceso legislativo. [2][3]

La Recomendación prevé que la Caja de Herramientas sea desarrollada por expertos de los Estados miembros reagrupados en el grupo de expertos eIDAS en estrecha coordinación con la Comisión y, en su caso, con otras partes interesadas de los sectores público y privado. [4]

[1] RECOMENDACIÓN (UE) 2021/946 DE LA COMISIÓN, de 3 de junio de 2021, relativa a un conjunto de herramientas comunes de la Unión para un enfoque coordinado hacia un marco europeo de identidad digital (DO L 210/51 de 14.6.2021)

[2] Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJOnding Reglamento (UE) No [3] /2014 por lo que respecta al establecimiento de un marco para una identidad digital europea, COM(2021) 281 final de 3.6.2021

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

Siguiendo el calendario indicativo establecido por la Recomendación, el grupo de expertos eIDAS acordó el proceso y los procedimientos de trabajo en su primera reunión, celebrada el 30 de septiembre de 2021, y debatió un documento oficioso sobre una descripción de alto nivel del ecosistema de la cartera de Identidad Digital de la Unión Europea (en lo sucesivo, «Cartera IDUE», o alternativamente, en inglés «EUDI Wallet» European Union Digital Identity Wallet) propuesto por la Comisión. [5]

Sobre esta base, el grupo de expertos decidió centrarse en primer lugar en una descripción más detallada del concepto de la Cartera IDUE, sus funcionalidades y aspectos de seguridad y en una serie de casos de uso básicos entre octubre y diciembre de 2021.

1.2 PROPÓSITO DEL DOCUMENTO

El presente esquema proporciona una descripción resumida de la comprensión del grupo de expertos eIDAS del concepto de Cartera IDUE, que incluye:

- objetivos de la Cartera IDUE,
- roles de los actores del ecosistema,
- los requisitos funcionales y no funcionales de la billetera y
- bloques de construcción potenciales.

El esquema no es obligatorio y presenta el estado de la situación del trabajo en curso del grupo de expertos eIDAS y no implica ningún acuerdo formal sobre su contenido o la propuesta de reglamento. Se complementará y actualizará en el proceso de establecimiento de la caja de herramientas. Se pretende desarrollar este esquema para convertirlo en un marco de arquitectura y referencia (MAR) completo del Marco Europeo de Identidad Digital (en inglés Architecture and Reference Framework. ARF), tal como se establece en la Recomendación. El MAR se ajustará al resultado de las negociaciones legislativas de la propuesta de Marco Europeo de Identidad Digital y consecuentemente se actualizará el presente documento.

El presente documento utiliza los términos "**deberá**[6]" y "**podrá**[7]" para expresar los requisitos actualmente previstos en la propuesta legislativa o las posibilidades no necesariamente propuestas como obligatorias, pero que no deben entenderse en el presente documento como formalmente prescriptivas o jurídicamente vinculantes.

Solo serán obligatorios el Reglamento marco europeo sobre la identidad digital adoptado definitivamente y los actos delegados y de ejecución finalmente adoptados en virtud de dicha base jurídica.

El grupo de expertos eIDAS adoptó el presente documento el 22 de febrero de 2022 y decidió publicarlo para recibir comentarios de las partes interesadas.

[5] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2021.210.01.0051.01.ESP

[6] Del inglés "shall": se utiliza para expresar requisitos obligatorios (disposiciones que deben seguirse). La forma negativa es "no deberá".

[7] Del inglés "may" se utiliza para expresar acciones permisibles (disposiciones que la implementación es capaz de seguir o no seguir). La forma negativa es "no es necesario".

2 OBJETIVOS DE LA CARTERA DE IDENTIDAD DIGITAL DE LA UNIÓN EUROPEA - IDUE (EUDIWallet)

El objetivo principal de la cartera europea de identidad digital propuesta es promover identidades digitales de confianza para todos los europeos, permitiendo a los usuarios tener el control de sus propias interacciones y presencia en línea. Se puede ver como una combinación de varios productos y servicios de confianza que permite a los usuarios solicitar, obtener y almacenar su información de forma segura, lo que les permite acceder a los servicios en línea, compartir datos sobre ellos y firmar / sellar documentos electrónicamente.

Una serie de casos de uso respaldarán el desarrollo de la Cartera IDUE para ofrecer de manera efectiva y sin problemas sus funcionalidades en todos los Estados miembros. El grupo de expertos de eIDAS ha trabajado en una serie de áreas de primeros casos de uso que incluyen:

- *Identificación segura y confiable para acceder a los servicios en línea*

Si bien la autenticación segura es una funcionalidad de la Cartera IDUE, las partes que confian (o partes informadas) que identifican a los usuarios con un conjunto definido de datos de identificación de personas con el fin de permitir el acceso a los servicios públicos y privados en línea es un caso de uso específico. Por ejemplo, las partes privadas de confianza aceptarán el uso de carteras EUDI cuando se les exija utilizar la autenticación reforzada de usuarios para la identificación en línea.

- *Movilidad y permiso* de *conducción* digital

La Cartera IDUE (EUDIWallet) puede acoger un permiso de conducción europeo totalmente digital para escenarios en línea y fuera de línea. Podría vincularse a una serie de certificaciones o testimonios adicionales ofrecidas por prestadores públicos o privados que cubran requisitos legales (por ejemplo, certificado o diploma de capacidad profesional) o requisitos y normas comerciales (por ejemplo, para el peaje de carreteras) en el área de transporte por carretera.

- *Salud*

El fácil acceso a los datos sanitarios es crucial tanto en contextos nacionales como transfronterizos. Basado en la experiencia del Certificado Covid Digital de la UE, la Cartera IDUE permitiría el acceso al historial sanitario del paciente, las recetas electrónicas, etc. [8]

- *Educación / Diploma*

Proporcionar documentos para los procedimientos de reconocimiento de cualificaciones puede ser costoso y llevar mucho tiempo para los usuarios finales, las empresas y los empleadores, las entidades de educación y formación y otras instituciones académicas. Por ejemplo, las certificaciones o testimonios de diplomas digitales podrían compartirse a través de las fronteras en un formato verificable, confiable y consumible a otra institución de educación o capacitación o a un posible empleador. La Cartera IDUE puede ser un repositorio de credenciales digitales educativas como testimonios electrónicos de atributos y un medio para intercambiarlos por parte de un alumno.

- *Finanzas Digitales*

La Cartera IDUE podría facilitar la autenticación de pagos con un alto grado de seguridad y permitir una experiencia sin fricciones en los pagos. En consonancia con la estrategia de pagos al por menor de la

[8] Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo, de 14 de junio de 2021, relativo a un marco para la emisión, verificación y aceptación de covid-1 interoperable9 certificados de vacunación, prueba y recuperación (Certificado DIGITAL COVID de la UE) para facilitar la libre circulación durante la pandemia de COVID-19

Comisión Europea, el caso de uso se desarrollaría en estrecha coordinación con los grupos consultivos de los Estados miembros sobre pagos al por menor y el sector financiero. [9]

Este trabajo puede ampliarse en el futuro a casos de uso adicionales.

[9] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO Y AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y EL COMITÉ DE LAS REGIONES sobre una estrategia de pagos al por menor para la UE COM/2020/592 final

3 ROLES EN EL ECOSISTEMA

Este capítulo establece una posible arquitectura del futuro ecosistema de la Cartera IDUE. Proporciona una base para que la discusión se actualice y complete en el curso del proceso definición de la caja de herramientas. El borrador de la arquitectura establece los diferentes roles y los flujos de proceso relevantes. Los roles potenciales del ecosistema de la Cartera IDUE se describen en la Figura 1.

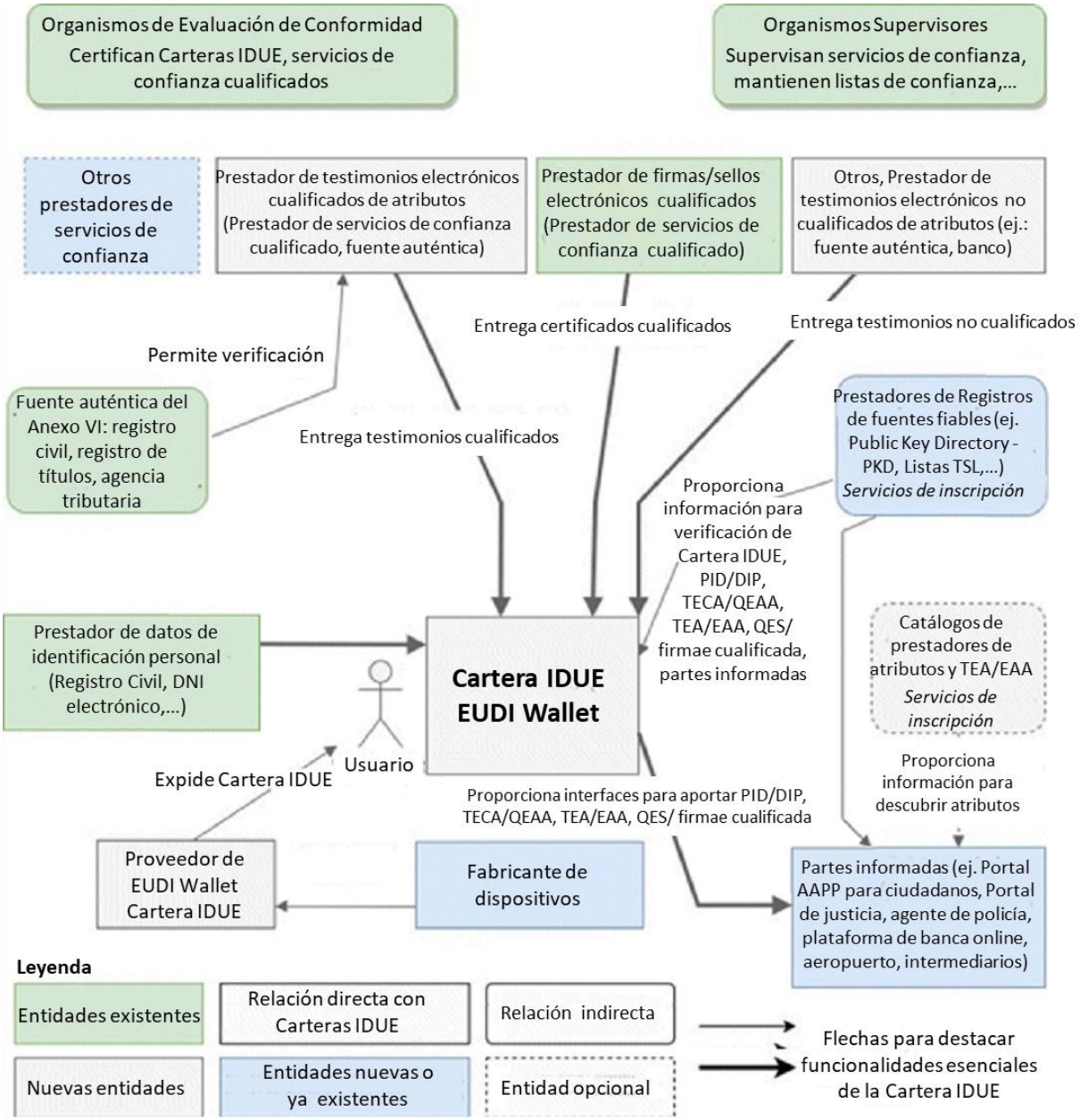


Figura 1 Descripción general de los roles de La Cartera IDUE

1 Usuarios finales de la Cartera IDUE
2 Emisores de carteras IDUE
3 Prestadores de datos de identificación de personas (DIP). En inglés, “Person Identification Data (PID) Providers”
4 Prestadores de registro de entidades confiables. En inglés “Providers of registries of trusted sources”
5 Prestadores de testimonios electrónicos cualificados de atributos (TECA). Partes informantes. En inglés “Qualified electronic attestation of attributes (QEAA) providers“
6 Prestadores de testimonios electrónicos de atributos (TEA) no cualificados. Partes informantes. En inglés “Non-qualified electronic attestation of attributes (EAA) providers”
7 Prestadores que emiten Certificados Cualificados y No Cualificados de firma electrónica o sello electrónico
8 Prestadores de otros servicios de confianza Cualificados y No Cualificados. En inglés “Providers of other trust services”
9 Fuentes fiables de información origen de su llevanza. En inglés “Authentic sources”
10 Partes que confían. Partes informadas. En inglés “Relying parties”
11 Organismos de evaluación de la conformidad (OEC). En inglés, “Conformity assessment bodies (CAB)”
12 Organismos Supervisores. En inglés, “Supervisory bodies”
13 Fabricantes de dispositivos y prestadores de subsistemas relacionados. En inglés, “Device manufacturers and related subsystems providers”
14 Prestadores de Catálogo de atributos y esquemas para el testimonio de atributos. En inglés, “Catalogue of attributes and schemes for the attestations of attribute providers “

A continuación, cada función se describe con más detalle sobre la base de la situación actual de los debates en el grupo de expertos de eIDAS.

Tenga en cuenta que la interfaz con un Prestador de Firma Electrónica Cualificada (QES, Qualified Electronic Signature/Seal) puede cubrir un proceso de firma electrónica local o remoto.

Esta descripción se actualizará y complementará en el curso de los trabajos sobre la caja de herramientas.

3.1 USUARIOS FINALES DE LA CARTERA IDUE

Los usuarios finales de La Cartera IDUE s se definen como personas físicas o jurídicas que utilizan la Cartera IDUE para recibir, almacenar y compartir testimonios (DIP, TECA, o TEA, e inglés PID, QEAA o EAA) y atributos particulares sobre el usuario, incluso para demostrar su identidad. La Cartera IDUE permitiría a los usuarios finales crear firmas y sellos electrónicos cualificados (QES).

Quién puede ser usuario de una cartera IDUE depende de la legislación nacional. El uso de una cartera IDUE por parte de los ciudadanos no sería obligatorio en virtud de la propuesta legislativa europea. Sin embargo, los Estados miembros estarían obligados a ofrecer la Cartera IDUE a sus ciudadanos.

3.2 EMISORES DE LA CARTERA IDUE

Los emisores de carteras IDUE son los Estados miembros u organizaciones, ya sea designadas o reconocidas por los Estados miembros, que ponen la Cartera IDUE a disposición de los usuarios finales.

Los términos y condiciones de la designación o el reconocimiento de la Cartera correspondería determinarlos a cada Estado Miembro.

La Cartera IDUE puede verse como una combinación de varios productos y servicios de confianza previstos en la propuesta legislativa europea, que en su conjunto otorgan al usuario el control exclusivo sobre el uso de sus datos de identificación personal (DIP/PID) y los testimonios electrónicos de atributos cualificadas o no cualificadas (TEA/EAA o TECA/QEAA), y cualquier otro dato personal dentro de su Cartera IDUE. Desde un punto de vista técnico, esto también puede implicar el control exclusivo del usuario 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 firma y el sello electrónicos.

Los emisores de carteras IDUE serían responsables de garantizar el cumplimiento de los requisitos aplicables a los carteras IDUE, en particular las definiciones pertinentes, funcionales y no funcionales, así como los requisitos de seguridad.

3.3 PRESTADORES DE DATOS DE IDENTIFICACIÓN PERSONAL (DIP)

Los prestadores de Datos de Identificación Personal (DIP, en inglés Providers of Person Identificación Data PID) verificarían la identidad del usuario de la Cartera IDUE , mantendrían una interfaz para proporcionar PID de forma segura a la Cartera IDUE (en un formato común armonizado) y pondrían a disposición de las partes que confían en la información para verificar la validez del PID, sin tener la capacidad de recibir ninguna información sobre el uso del PID. Las condiciones de estos servicios corresponderían a cada Estado miembro determinarlas. [10]

Los prestadores de DIP(PID pueden ser, por ejemplo, las mismas organizaciones que hoy en día emiten documentos de identidad oficiales, medios de identidad electrónica, emisores de la Cartera IDUE , etc. Los emisores de Carteras IDUE pueden o no ser las mismas organizaciones que los prestadores de DIP/PID.

3.4 PRESTADORES DE REGISTRO DE ENTIDADES CONFIABLES

Es posible que sea necesario verificar el estado específico de un rol en **el ecosistema de** la Cartera IDUE de manera confiable. Tales roles **pueden** ser:

- Emisores de la Cartera IDUE
- Prestadores de datos de identificación de personas
- Prestadores de testimonio electrónico cualificado de atributos (TECA/QEAA). Partes informantes.
- Prestadores cualificados que expiden Certificados cualificados para firma/sello electrónico
- Partes informadas.
- Prestadores de testimonio electrónico de atributos (TEA/EAA) no cualificado. Partes informantes.
- Prestadores que expiden Certificados no cualificados para firma/sello electrónico
- Prestadores de otros servicios de confianza
- Prestadores de Catálogo de atributos y esquemas para el testimonio de atributos

[10] Sin perjuicio del mecanismo real de forma de facilitar la información, incluso si es directa o indirectamente

Otros roles pueden ser necesarios y, por lo tanto, deben definirse y mencionarse explícitamente dependiendo del rol específico y su criticidad, por ejemplo, los diferentes roles y actores involucrados en los procesos de firma electrónica remota.

Los registros de entidades confiables[11] prestarán un servicio de inscripción para cada tipo de entidad según su rol, como partes informantes y partes informadas, mantendrán actualizado el registro pertinente y permitirán el acceso de terceros a la información que gestionan. Los términos y condiciones aplicables a las entidades que se registren los determinaría cada registrador, a menos que se especifique, por ejemplo, en normas sectoriales.

Por ejemplo, el estatus cualificado de los Prestadores Cualificados de Servicios de Confianza (PCSC) en inglés, Qualified Trust Services Providers (QTSP) y el servicio de confianza cualificado que prestan ya se registran en listas de confianza TSL de los Estados miembros. Otras informaciones (como la prestación de testimonios TECA/QEAA) y otros roles pueden proporcionarse en otras formas de registros de confianza.

3.5 PRESTADORES DE TESTIMONIO ELECTRÓNICO CUALIFICADO DE ATRIBUTOS

Los TEA/EAA cualificados los prestarían PCSC/QTSP. El marco de confianza para PCSC/QTSP se aplicaría también a TECA/QEAA. Los prestadores de TECA/QEAA mantendrían una interfaz para solicitar y proporcionar TECA/QEAA, incluida una interfaz de autenticación mutua con la Cartera IDUE y potencialmente una interfaz hacia fuentes fiables de información origen de su llevanza para verificar atributos. Los prestadores de TECA/QEAA estarían obligados a proporcionar información o la ubicación de los servicios que se pueden utilizar para preguntar sobre el estado de validez del TECA/QEAA, sin tener la capacidad de recibir ninguna información sobre el uso de los testimonios. Los términos y condiciones de estos servicios los determinaría cada PCSC/QTSP, más allá de lo especificado en el Reglamento eIDAS.

3.6 PRESTADORES DE TESTIMONIO ELECTRÓNICO DE ATRIBUTOS NO CUALIFICADO

Cualquier prestador de servicios de confianza (PSC) puede proporcionar TEA/EAA no cualificado. Si bien estarían sujetos a supervisión bajo eIDAS, se puede suponer que otros marcos legales o contractuales distintos de eIDAS gobernarían principalmente las reglas para la provisión, uso y reconocimiento de TEA/EAA. Estos otros marcos pueden cubrir áreas de políticas como permisos de conducir, credenciales educativas, pagos digitales, aunque también pueden depender de prestadores cualificados de testimonio electrónico cualificado de atributos. Para que se utilice TEA/EAA, los Prestadores de Servicios de Confianza PSC/TSP (en inglés Trust Service Provider) tendrían que ofrecer a los usuarios una forma de solicitar y obtener TEA/EAA, lo que significa que tendrían que cumplir técnicamente con las especificaciones de la interfaz de la Cartera IDUE. Dependiendo de las reglas de dominio, los prestadores de TEA/EAA pueden proporcionar información de validez sobre los TEA/EAA, sin tener la capacidad de recibir ninguna información sobre el uso de TEA/EAA. Los términos y condiciones de emisión de TEA/EAA y los servicios relacionados estarían sujetos a normas sectoriales.

[11] Más adelante se entra en detalle sobre los registros confiables.

3.7 PRESTADORES QUE EMITEN CERTIFICADOS CUALIFICADOS Y NO CUALIFICADOS DE FIRMA ELECTRÓNICA O SELLO ELECTRÓNICO

El artículo 6 bis, apartado 3, de la COM(2021)281 final exige que la Cartera EUDI permita al usuario firmar mediante firma o sello electrónico cualificado. Este objetivo se puede alcanzar de varias maneras:

- La Cartera IDUE puede incluir un dispositivo cualificado de creación de firma/sello (DCCF/DCCS/QSCD), en inglés Qualified Seal/Signature Creation Device o
- La Cartera IDUE puede actuar como una herramienta de autenticación segura como parte de un DCCF/DCCS/QSCD local o remoto administrado por un PCSC/QTSP.

La Cartera EUDI también puede permitir al usuario firmar mediante certificados de persona física o jurídica no cualificados o mediante certificados de persona física o jurídica cualificados sin hacer uso de Dispositivos Cualificados DCCF/DCCS/QSCD.

3.8 PRESTADORES DE OTROS SERVICIOS DE CONFIANZA CUALIFICADOS Y NO CUALIFICADOS

Los prestadores de otros servicios de confianza cualificados o no cualificados, como sellos de tiempo, pueden interactuar con la Cartera IDUE. Los detalles de este rol o roles en el ecosistema de Cartera IDUE están sujetos a un mayor debate.

3.9 FUENTES FIABLES DE INFORMACIÓN ORIGEN DE SU LLEVANZA

Las fuentes *fiables de información origen de su llevanza* serían los repositorios o sistemas públicos o privados reconocidos por la ley o que la ley determine su reconocimiento por las partes que confían (partes informadas) y que contienen atributos de una persona física o jurídica. Las *fuentes auténticas* (*fuentes fiables de información origen de su llevanza*) en el ámbito de aplicación del **Anexo VI** de la propuesta legislativa europea son fuentes de atributos relativos a: dirección, edad, sexo, estado civil, composición familiar, nacionalidad, títulos, diplomas de cualificaciones de educación y formación, títulos y licencias de cualificaciones profesionales, permisos y licencias públicos, datos financieros y de empresas. Se requeriría que las fuentes *fiables de información origen de su llevanza* en el ámbito de aplicación del **Anexo VI** proporcionaran interfaces a los prestadores de TECA/QEAA para verificar la autenticidad de los atributos reseñados, ya sea directamente o a través de intermediarios designados admitidos a nivel nacional. Para este propósito, las fuentes *fiables de información origen de su llevanza* pueden necesitar mantener una interfaz para recoger la autorización que el usuario presta para que los prestadores de TECA/QEAA puedan acceder a los datos de la persona. Las sinergias con el sistema técnico de una sola vez del Reglamento sobre el portal digital único (Once Only Technical System of the Single Digital Gateway Regulation[12]) se considerarán un medio para lograrlo. Correspondería a los Estados miembros determinar las condiciones de la prestación de estos servicios.

Las entidades que realizan la llevanza de constancias gestionan la información que corresponde a sus atribuciones y permiten a terceros el acceso a la información de la que son la fuente primaria. La información registrada corresponde a la actividad de la entidad (según sus propios términos y condiciones) y puede estar sujeta a normas sectoriales.

[12] https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Once+Only+Technical+System

3.10 PARTES INFORMADAS.

Las Partes que confían en la información que reciben (*partes informadas*) son personas físicas o jurídicas que admiten y dan valor a una identificación electrónica o un servicio de confianza. En el contexto de la Cartera IDUE, solicitarían los atributos que requirieran contenidos en el conjunto de datos DIP/PID, TECA/QEAA y TEA/EAA a los usuarios de la Cartera IDUE con sujeción a su aceptación por parte del titular de la cartera y dentro de los límites de la legislación y las normas aplicables. La razón de que se confía en la cartera EUDI por una entidad que requiere de ciertas datos de atributos del usuario de la cartera puede ser un requisito legal, un acuerdo contractual o por otros motivos. Para confiar en la Cartera EUDI, las partes que confían (*partes informadas*) tendrían que informar al Estado miembro en el que están establecidas y su intención de hacerlo. Las partes que confian (*partes informadas*) tendrían que mantener una interfaz con la Cartera IDUE para solicitar testimonios con técnicas de autenticación mutua. Las partes que confian (*partes informadas*) son responsables de llevar a cabo el procedimiento para autenticar los testimonios que reciben de la Cartera IDUE.

Las partes que confian (*partes informadas*) pueden interactuar con La Cartera IDUE a través de proxies o puertas de enlace como, por ejemplo, pasarelas de autenticación nacionales o prestadores de servicios de autenticación del sector privado.

3.11 ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD (OEC).

Las carteras EUDI tendrían que estar certificadas por organismos públicos o privados acreditados designados por los Estados miembros. Los PCSC/QTSP deben ser auditados regularmente por Organismos de Evaluación de la Conformidad (OEC), en inglés, Conformity Assessment Bodies (CABs). Los OEC/CAB estarían acreditados por las Entidades de Acreditación de los Estados miembros como responsables de llevar a cabo evaluaciones en las que los Estados miembros tendrán que confiar antes de emitir una cartera EUDI o proporcionar el estatus cualificado a un Prestador de Servicios de Confianza. Las normas y esquemas utilizados por los OEC(CAB para cumplir sus tareas se especificarían más adelante en el proceso de elaboración de la Caja de Herramientas. [13]

3.12 ORGANISMOS SUPERVISORES

Los organismos de supervisión designados por los Estados miembros se notificarán por estos a la Comisión Europea. Estos organismos llevarán a cabo la supervisión de los PCSC/QTSP y, en caso necesario, adoptarán medidas en relación con los prestadores de servicios de confianza no cualificados. Los organismos de supervisión, según el enfoque, pueden necesitar asignar recursos adicionales para cumplir con sus responsabilidades y diseñar procesos relevantes, como la presentación de informes o la realización de evaluaciones de riesgos.

3.13 FABRICANTES DE DISPOSITIVOS Y PRESTADORES DE SUBSISTEMAS RELACIONADOS

La Cartera IDUE dispondrá de una serie de interfaces con los dispositivos en los que se basan, que pueden ser para los siguientes propósitos:

- Almacenamiento local
- Acceso a Internet en línea

[13] Artículo 6 c, apartado 3

- Sensores como cámara de smartphone, sensores IR, micrófonos, etc.
- Canales de comunicación fuera de línea como Bluetooth low energy (BLE), WIFI Aware, Near Field Communication (NFC)
- Emisores como pantallas, linternas, altavoces, etc.

Para el almacenamiento seguro de material criptográfico, se pueden interactuar dispositivos o servicios específicos. Otras entidades relacionadas pueden ser prestadores de servicios, como prestadores de servicios en la nube, prestadores de tiendas de aplicaciones, etc.

La propuesta legislativa europea establece restricciones (por ejemplo, el cumplimiento de un nivel de garantía elevado) para las que se pueden utilizar tipos de dispositivos y servicios a efectos de la emisión de la Cartera EUDI. Del mismo modo, la disponibilidad, así como los términos y condiciones de los prestadores de interfaz de dispositivos y prestadores de servicios relacionados establecerán restricciones adicionales para los emisores de la Cartera IDUE.

3.14 PRESTADORES DE CATÁLOGO DE ATRIBUTOS Y ESQUEMAS PARA EL TESTIMONIO DE ATRIBUTOS

Los prestadores de TECA/QEAA y TEA/EAA pueden publicar información relevante sobre los testimonios que proporcionan en un catálogo o en varios catálogos. Potencialmente permitiría a otras entidades, como las partes que confían, descubrir los atributos y esquemas que se proporcionan, y cómo validarlos / verificarlos y también diferenciar entre tipos de testimonios electrónicos cualificados de atributos. La Comisión Europea está obligada a establecer las especificaciones técnicas mínimas, las normas y los procedimientos a tal efecto.

4 REQUISITOS FUNCIONALES

Este capítulo proporciona una visión general de los requisitos funcionales de La Cartera IDUE. Sobre la base de la propuesta legislativa europea, las carteras EUDI proporcionarán las siguientes funcionalidades, que se explican con más detalle en los respectivos subcapítulos:

1. Realizar la identificación electrónica, almacenar y gestionar la certificación electrónica cualificada de atributos (TECA/QEAA) y la certificación electrónica de atributos (TEA(EAA) **de forma local o remota;**
2. Solicitar y obtener de los testimonios de los prestadores, la certificación electrónica cualificada de atributos (TECA/QEAA) y la certificación electrónica de atributos (TEA/EAA);
3. Proporcionar o acceder a funciones criptográficas;
4. Autenticación mutua entre la Cartera IDUE y entidades externas;
5. Seleccionar, combinar y compartir con las partes que confian (*entidades informadas*) DIP/PID, TECA/QEAA y TEA/EAA;
6. Interfaz de usuario que gestiona el consentimiento informado del usuario y un mecanismo de autorización explícita;
7. Firma de datos mediante un certificado cualificado dando lugar a una firma/sello electrónico cualificado (QES);
8. Disponibilidad de interfaces accesibles para terceros.

La Figura 2 proporciona una visión general de las funcionalidades de La Cartera IDUE como bloques funcionales. Los bloques se dividen en cinco categorías: interfaz de usuario (en azul), almacenamiento de datos (en amarillo), funciones complejas / protocolos criptográficos (en morado), material criptográfico sensible (en rojo) y módulo de medios de identificación electrónicos eID (contorno verde). Algunas funcionalidades las proporciona la propia Cartera IDUE y otras se pueden prestar por un subsistema de la Cartera IDUE o por una entidad externa a través de una interfaz.

Tenga en cuenta que la interfaz QES puede dar cobertura a un proceso de firma electrónica local o remoto.

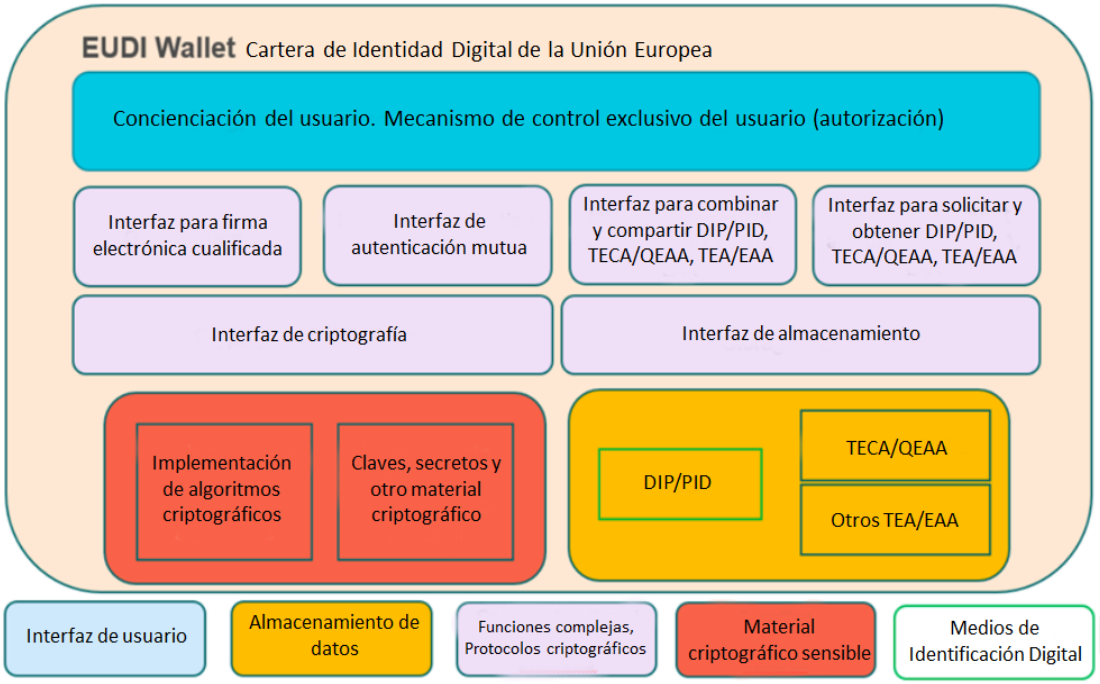


Figura 2 Funcionalidades de la Cartera EUDI

Este capítulo diferencia entre funciones e interfaces obligatorios (**deberán**/"**shall**") siguiendo la propuesta legislativa europea y funciones e interfaces opcionales adicionales que pueden ser útiles o deseables (**podrán/"may").** Esta diferenciación está sujeta a actualización y finalización en el curso de la labor del grupo de expertos sobre la caja de herramientas.

4.1 ALMACENAR DATOS DE IDENTIFICACIÓN DE PERSONA, TESTIMONIO ELECTRÓNICO CUALIFICADO DE ATRIBUTOS Y TESTIMONIO ELECTRÓNICO DE ATRIBUTOS

La interfaz de almacenamiento de la Cartera IDUE tiene como objetivo ofrecer una capacidad de almacenamiento para los datos recibidos de identificación de persona, TECA/QEAA y TEA/EAA para que el usuario pueda compartirlos con las partes que confían (*partes informadas*), sin requerir solicitudes de TECA/QEAA, TEA/EAA o DIP/PID cada vez que se necesite la información. Esto reduce la capacidad del proveedor de testimonios electrónicos para rastrear el uso de testimonios electrónicos proporcionados por el usuario.

Como se indica en la propuesta legislativa europea, el almacenamiento de la Cartera IDUE puede ser local (ubicado en un dispositivo que posea el usuario) o remoto (en una infraestructura alojada en la nube) [14]. La cartera EUDI **tendrá** o bien solo almacenamiento local o bien almacenamiento híbrido con al menos punteros a un almacenamiento remoto que se almacenen de forma lcal. Dependiendo de las opciones de implementación técnica, **puede** ser necesario copiar, sincronizar y/o mover datos entre diferentes componentes de almacenamiento, locales o remotos.

4.2 SOLICITAR Y OBTENER DATOS DE IDENTIFICACIÓN DE PERSONA, TESTIMONIO ELECTRÓNICO CUALIFICADO DE ATRIBUTOS Y TESTIMONIO ELECTRÓNICO DE ATRIBUTOS

La Cartera EUDI **deberá:**

- integrar una funcionalidad para solicitar y obtener DIP/PID del usuario durante el registro inicial, por ejemplo, a través de una interfaz con identificaciones electrónicas de medios de aseguramiento de nivel alto nivel; [15]
- permitir al usuario solicitar y obtener TEA/EAA cualificadas y no cualificadas, a través de una interfaz con prestadores (cualificados y no cualificados) de TEA/EAA;
- permitir que el usuario elimine, por ejemplo, TEA/EAA, TECA/QEAA, DIP/PID, material criptográfico, etc. de la Cartera.

La Cartera EUDI **puede**:

[14] En el escenario de almacenamiento remoto, el uso compartido sin conexión del PID y (Q)EAA presentará desafíos adicionales que requieren un mínimo en el almacenamiento del dispositivo.

[15] Tal como se define en el Reglamento de Ejecución de la Comisión Reglamento (UE) 2015/1502, de 8 de septiembre de 2015, por el que se establecen especificaciones técnicas y procedimientos mínimos para los niveles de garantía de los medios de identificación electrónica con arreglo al artículo 8, apartado 3, del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo de Identificación Electrónica y Servicios de Confianza para las Transacciones Electrónicas en el Mercado Interior.

[14] Ibíd., la lista descrita no es exhaustiva.

- confiar, para su uso durante el proceso de identificación/autenticación electrónica, en una interfaz con fuentes auténticas[14], tales como documentos de identidad oficiales (por ejemplo, a través de un acceso a la interfaz NFC de teléfonos móviles para leer documentos de identidad que equipen un chip NFC) o registros civiles.

4.3 FUNCIONES CRIPTOGRÁFICAS

El acceso seguro a las funciones criptográficas almacenadas local o externamente será necesario para implementar la mayoría de las funcionalidades de la Cartera IDUE (por ejemplo, firma electrónica cualificada (FEC/QES), autenticación, divulgación selectiva). En el caso de funciones criptográficas almacenadas externamente, la cartera proporcionará un conjunto mínimo de funciones criptográficas locales que permitan un acceso seguro a ellas. Los métodos y funciones criptográficos globales **deberán** cumplir los requisitos existentes y futuros originados en normas, actos de ejecución europeos y certificaciones basados en estos.

Estas funciones **deberán** ser usadas para gestionar:

- identificación electrónica del usuario a las partes que confían;
- autenticación de TEA/EAA, TECA/QEAA, DIP/PID cuando estén vinculados al cartera EUDI;
- autenticación de la propia cartera EUDI frente a terceros;
- el medio de activación para el DCCF/QSCD remoto, si la Cartera IDUE se basa en un DCCF/QSCD remoto para su funcionalidad de firma electrónica cualificada (FEC/QES);
- los certificados cualificados y sus claves criptográficas, si la Cartera IDUE se basa en un DCCF/QSCD local para su funcionalidad de firma electrónica cualificada (FEC/QES);
- el medio de acceso al almacenamiento remoto de la Cartera IDUE si la Cartera IDUE hace uso de almacenamiento remoto;
- en su caso, almacenamiento seguro de datos personales sensibles en el dispositivo.

Estas funciones **pueden** ser utilizadas para gestionar:

- autenticación del usuario en forma de seudónimo frente a partes que confían.

4.3.1 Gestión de material criptográfico

La gestión de material criptográfico de la Cartera IDUE proporciona la capacidad de generar, almacenar, usar, modificar y eliminar material criptográfico. Dependiendo de la sensibilidad del material criptográfico, la interfaz de gestión criptográfica **puede** aprovechar las soluciones de software y/o hardware para proporcionar la funcionalidad.

Los algoritmos admitidos **deberán** ser lo suficientemente sólidos en términos de criptografía para garantizar la confidencialidad, la integridad y la autenticidad. Dicha determinación podrá concluirse mediante su inclusión en, por ejemplo, el Catálogo SOG-IS.

4.3.2 Entornos de confianza

Ciertos cálculos requieren un nivel adicional de confianza, que puede no ser proporcionado por los entornos de ejecución de software estándar. En esos casos, la Cartera IDUE **puede** confiar en un entorno de ejecución de confianza (Trusted Execution Environment, TEE) y elementos seguros (Secure Elements, SE) localmente o en una tecnología remota equivalente o similar, dependiendo del dispositivo para ejecutar esos cálculos.

Se definirán los medios de identificación para hacer cumplir un estándar común para acceder a un TEE o SE en la Cartera IDUE, ya que proporcionará un mayor nivel de confianza a toda la implementación.

4.4 AUTENTICACIÓN MUTUA

Para garantizar acciones informadas del usuario y niveles de seguridad adecuados, la Cartera IDUE implementará capacidades de autenticación mutua. La capacidad de identificación y autenticación mutuas [16]**abarcará** tanto el extremo de la Cartera EUDI como el extremo del tercero, ya que, según el caso de uso, la Cartera EUDI **podrá** identificarse y autenticarse a sí misma o al usuario, Sin embargo, deberá ser capaz de identificar y autenticar al tercero con el que está interactuando. Además, esta identificación y autenticación mutuas **deberán** ser posibles tanto en línea (a través de Internet) como fuera de línea (sin conexión).

Para garantizar que la cartera EUDI pueda ser utilizada de manera fluida tanto por los PSC/TSP como por las partes que confían, se **deberá** especificar un protocolo de autenticación común que garantice la interoperabilidad al menos a nivel de la UE/EU y tenga en cuenta las normas europeas o internacionales pertinentes.

4.4.1 Identificación y autenticación de la Cartera IDUE/EUDI Wallet

La propia cartera IDUE/EUDI deberá poder demostrar a la parte que confía tanto el origen como la integridad de la Cartera EUDI individual que se utilice y contribuir así a aumentar la confianza y la seguridad del ecosistema. Esto **demostrará** que se ha realizado una certificación válida y que la solución se ha instalado en un dispositivo adecuado con la seguridad adecuada. Además, se deberán realizar comprobaciones de revocación.

4.4.2 Identificación y autenticación de terceros con los que interactúe la Cartera IDUE/EUDI

Por razones de seguridad y transparencia, la Cartera EUDI **deberá** tener la capacidad de identificar y autenticar a terceros con los que interactúe, en particular:

- prestadores de servicios de confianza cualificados y no cualificados (PSC/TSP);
- partes que confian, incluidos los agentes intermedios y pasarelas;
- el emisor de la Cartera IDUE.

La Cartera IDUE **puede** admitir varios protocolos de varios estándares de autenticación reconocidos. Se definirían reglas y procesos de gobernanza para agregar y eliminar protocolos de la lista de estándares admitidos.

4.5 SELECCIÓN, COMBINACIÓN Y PUESTA EN COMÚN DE LOS DATOS DE IDENTIFICACIÓN DE LA PERSONA, TESTIMONIO ELECTRÓNICO CUALIFICADO DE ATRIBUTOS Y TESTIMONIO ELECTRÓNICO DE ATRIBUTOS

La propuesta legislativa europea establece que la Cartera EUDI es un medio de identificación electrónica. Por lo tanto, la Cartera EUDI **será** capaz de realizar la identificación y autenticación del usuario con un conjunto específico de DIP/PID, realizando así la identificación con fuerza legal cuando sea necesario.

[16] La autenticación mutua entre carteras y partes informadas no debe entenderse como obligatoria para cada transacción.

La cartera **aprovechará** un protocolo común para la identificación y el intercambio de atributos, incluida la verificación de la integridad y autenticidad de la información, independientemente del conjunto de atributos compartidos, con el fin de reducir la complejidad técnica de la solución y facilitar su implementación. Esta funcionalidad se basará en TECA/QEAA y TEA/EAA, las estructuras de datos de esos testimonios y su protocolo de intercambio reutilizado para DIP/PID.

La funcionalidad puede tener en cuenta la infraestructura y las funciones de eIDAS existentes para respaldar un funcionamiento sin problemas de la Identidad Digital de la Unión Europea y los medios de identificación electrónica existentes.

La Cartera EUDI **imposibilitará** la recopilación de información sobre el uso de la Cartera que no sea necesaria para la prestación de los servicios del Cartera, ni combinará los datos de identificación personal y cualquier otro dato personal almacenado o relacionado con el uso de la Cartera de Identidad Digital de la Unión Europea con datos personales de cualquier otro servicio ofrecido por su emisor o de servicios de terceros que no sean necesarios para la prestación del servicios de la Cartera, salvo que el usuario lo haya solicitado expresamente.

La Cartera EUDI **forzará** el cumplimiento de la privacidad desde el diseño y la divulgación selectiva de atributos.

La divulgación selectiva y la combinación de testimonios se pueden manejar de dos maneras diferentes:

- La Cartera IDUE puede contener una colección muy amplia de atributos como DIP/PID, TECA/QEAA y TEA/EAA, y cada vez que se requiere un atributo específico o la derivación de un atributo específico, se debe solicitar un nuevo DIP/PID, TECA/QEAA o TEA/EAA a los prestadores.
- La cartera EUDI puede tener la capacidad intrínseca, basada en el DIP/PID obtenido y los TECA/QEAA y TEA/EAA, para divulgar selectivamente, derivar un atributo específico y agregar varios atributos individuales, sin la necesidad de nuevos DIP/PID, TECA/QEAA o TEA/EAA o interacciones con los prestadores DIP/PID, TECA/QEAA y TEA/EAA. Por ejemplo, la adecuación de esquemas de firma electrónica específicos asociados a DIP/PID, TECA/QEAA y TEA/EAA podrían habilitar tales capacidades.

El uso compartido de testimonios se puede dividir en dos tipos: uso compartido sin conexión y en línea.

4.5.1 Uso compartido sin conexión

El escenario de uso compartido sin conexión corresponde a un caso de uso en el que el usuario comparte un DIP/PID, TECA/QEAA o TEA/EAA o una combinación de estos a un tercero, que se encuentra en las proximidades inmediatas. Si el testimonio electrónico no está vinculada a la Cartera IDUE, el tercero podrá solicitar datos adicionales fuera del ámbito de aplicación de la Cartera IDUE. Por ejemplo:

- para garantizar la validación adecuada de un *certificado sanitario* de la UE, el tercero requeriría un documento de identidad con información biométrica, como una fotografía, como prueba de que el titular del *certificado sanitario* de la UE es el propietario legítimo del certificado;[17]

[17] La identificación adicional de las personas que muestran este tipo de *certificados sanitarios* es específicamente relevante cuando su información está destinada a ser utilizada fuera del sector de la salud.

- una prueba de edad podría proporcionar la edad y la fotografía de un usuario, ambas autenticadas por una autoridad de confianza. En ese caso, el verificador puede verificar físicamente que la fotografía coincide con el usuario, sin ningún vínculo entre la prueba de edad y la billetera EUDI, que, en este escenario, solo proporcionaría capacidades de almacenamiento y uso compartido.

Si los datos DIP/PID, TECA/QEAA o TEA/EAA están vinculados a la Cartera EUDI, el titular de la Cartera EUDI podrá demostrar que estos datos son objeto de los atributos atestiguados. Esto evita la necesidad de que el usuario proporcione información de identificación adicional a la parte de confianza. [18]

4.5.2 Uso compartido en línea

El uso compartido en línea requerirá que el usuario demuestre la propiedad de la DIP/PID, TECA/QEAA o TEA/EAA utilizada demostrando el acceso y el control sobre el material criptográfico vinculado a la DIP/PID, TECA/QEAA o TEA/EAA, si es necesario para el escenario de uso.

El protocolo de autenticación **será** lo más común posible para reducir la complejidad general de la solución y facilitar la adopción de la Cartera EUDI. Este protocolo sería tal que pueda cumplir con los requisitos pertinentes de nivel de aseguramiento alto y puede incluir una consideración de las infraestructuras de autenticación existentes cuando sea pertinente. El objetivo de un protocolo de autenticación común entre la Cartera IDUE y terceros no excluye la existencia de diferentes soluciones subyacentes para proporcionar, verificar y revocar DIP/PID, TECA/QEAA o TEA/EAA. [19][20]

4.6 INTERFAZ DE USUARIO PARA EL APERCIBIMIENTO INFORMADO DEL USUARIO Y EL MECANISMO DE AUTORIZACIÓN

La interfaz de usuario de la Cartera IDUE cubre dos funcionalidades principales, la información al usuario y su autorización. Ambos son necesarios en el contexto de la identificación, autenticación, firma electrónica y compartición de testimonios.

4.6.1 Componente de apercibimiento informado del usuario

La Cartera EUDI **deberá**:

- mostrar información clara e inequívoca al usuario para permitir decisiones debidamente informadas.
  En particular, se informará claramente al usuario:
  - De la identidad de las diferentes partes con las que el usuario interactuará[21]
  - De la razón para compartir un testimonio electrónico del atributo, incluido quién lo está preguntando, qué atributos se solicitan y para qué propósito según lo definido por la parte informada;
  - Del tipo de operación que se está ejecutando.

[18] Será necesario discutir si este enlace requiere directa o indirectamente una inclusión de material criptográfico sobre el que el titular de la cartera EUDI pueda demostrar que está bajo su control.

[19] según el Reglamento de Ejecución CIR 2015/1502

[20] El presente protocolo común tendrá por objeto normalizar la estructuras de datos, las secuencias de mensajes entre las partes y los mecanismos criptográficos subyacentes

[21] Prestadores de servicios de confianza cualificados, partes informadas, emisores de carteras, registros confiables, otros carteras IDUE, etc.

- De sus derechos de protección de datos de carácter personal en virtud del RGPD (Reglamento General de Protección de Datos).

- permitir que el usuario identifique los atributos que la parte informada requiere como obligatorios y, si corresponde, los atributos que la parte informada considera opcionales;
- mostrar una "marca de confianza de la Cartera de Identidad Digital de la UE" para el usuario;
- mostrar para la firma electrónica cualificada:
  - quién la pide,
  - qué documento hay que firmar,
  - qué política de firma electrónica se debe aplicar, etc.;
- mostrar los eventos relacionados con el uso de su Cartera EUDI (por ejemplo, mediante notificación o visualización del historial de eventos de la Cartera IDUE).

Además, la Cartera EUDI **puede**:

- integrar un código de "coacción"[22];
- validar TEA/EAA cualificadas (TECA/QEAA) y EEA no cualificadas;
- conceder al usuario una forma inequívoca de distinguir entre TEA/EAA cualificadas y no cualificadas, así como su estado de validez *(por ejemplo, mediante el uso de un indicador visual similar a la marca europea de confianza al mostrar* TEA/EAA *cualificadas);*
- restringir el uso compartido de ciertos conjuntos de atributos con ciertas partes, o advertir al usuario que la parte informada puede no estar autorizada a acceder a estos atributos o solicitarlos[23].

4.6.2 Mecanismo de autorización de usuario

Con el fin de proteger la privacidad del usuario y garantizar el control exclusivo del usuario sobre su cartera EUDI (incluidos los datos personales y los atributos), la Cartera EUDI **deberá**:

- confiar en un mecanismo de autorización armonizado que garantice la seguridad y la privacidad desde el diseño;
- obtener y almacenar las autorizaciones de usuario para realizar las acciones que se solicitan. Esto implica una acción específica del usuario, incluida una operación activa que demuestre que el usuario legítimo está expresando su consentimiento. [24]
- garantizar que la autorización del usuario con respecto a la creación de una firma electrónica cualificada se gestionará como parte del dispositivo cualificado de creación de firma/sello (DCCF/QSCD/DCCS) en el que se basa la Cartera IDUE. [25]

[22] Un código de "coacción" es un código alternativo que se debe usar cuando el usuario está actuando bajo coacción, que tiene la apariencia de que se usa el código real, pero que activaría una alerta o bloquearía la transacción que se está realizando.

[23] Estas "políticas de intercambio" pueden definirse a diferentes niveles.

[24] La autorización del usuario puede significar tener control total (1) sobre el DIP/PID, TECA/QEAA o TEA/EAA divulgado, a través de la capacidad de seleccionar, combinar, compartir o rechazar el intercambio de atributos solicitados a un tercero identificado, en línea o fuera de línea; (2) durante el proceso QES (firma electrónica cualificada), a través de la posibilidad de acceder al documento así como la política de firma electrónica y las implicaciones previas a la realización de la firma electrónica.

Además, la Cartera IDUE **exigirá** al usuario que utilice la autenticación de dos factores en una combinación de al menos dos factores de autenticación para determinados casos de uso, cumpliendo los requisitos de Nivel de Aseguramiento (Level of Assurance) alto:

- una prueba de conocimiento (”algo que sabes”);
- una prueba de posesión (”algo que tienes”);
- una prueba de inherencia (biometría o comportamientos) (”algo que eres”);

4.7 FIRMAS Y SELLOS ELECTRÓNICOS CUALIFICADOS MEDIANTE DISPOSITIVOS CUALIFICADOS DE GESTIÓN DE CLAVES PRIVADAS

Al utilizar la Cartera EUDI, **será** posible realizar procesos de firma que resulten en una firma electrónica (persona física) o en un sello electrónico (persona jurídica). Un usuario de la Cartera IDUE **podrá** crear firmas electrónicas y sellos electrónicos cualificados y no cualificados, ya sea a través de:

- La Cartera actuando como un DCCF/QSCD/DCCS;
- El uso de un DCCF/QSCD/DCCS local externo a la cartera pero disponible como funcionalidad principal del dispositivo que aloja la Cartera;
- A través de una interfaz con un servicio cualificado para la gestión de DCCF/QSCD/DCCS remotos. En este caso, la cartera EUDI permitirá al usuario activar su clave privada con la que realizar firmas o sellos electrónicos.

4.8 INTERFACES CON ENTIDADES EXTERNAS

Además de las funcionalidades enumeradas anteriormente, la Cartera IDUE deberá incluir ciertas interfaces con entidades externas a las que deberán aplicarse requisitos, especificaciones y estándares específicos, por dearrollar. Se presentan en la Figura 3 a continuación.

Representadas en verde, se recogen las interfaces de la Cartera IDUE que deberán definirse en especificaciones técnicas futuras. Estas interfaces afectarán al diseño de los componentes de la Cartera IDUE y deberán especificarse en la etapa inicial del diseño del prototipo de la Cartera IDUE .

Tenga en cuenta que la interfaz de firma electrónica cualificada puede dar cobertura a un proceso de firma electrónica local o remoto.

[25] Cuando el mecanismo de consentimiento armonizado proporcionado por EUDI Wallet (Cartera IDUE) se utiliza, por conveniencia, para crear QES (firma electrónica cualificada), puede ser certificado como parte del QSCD (DCCF, Dispositivo Cualificado de Creación de Firma).

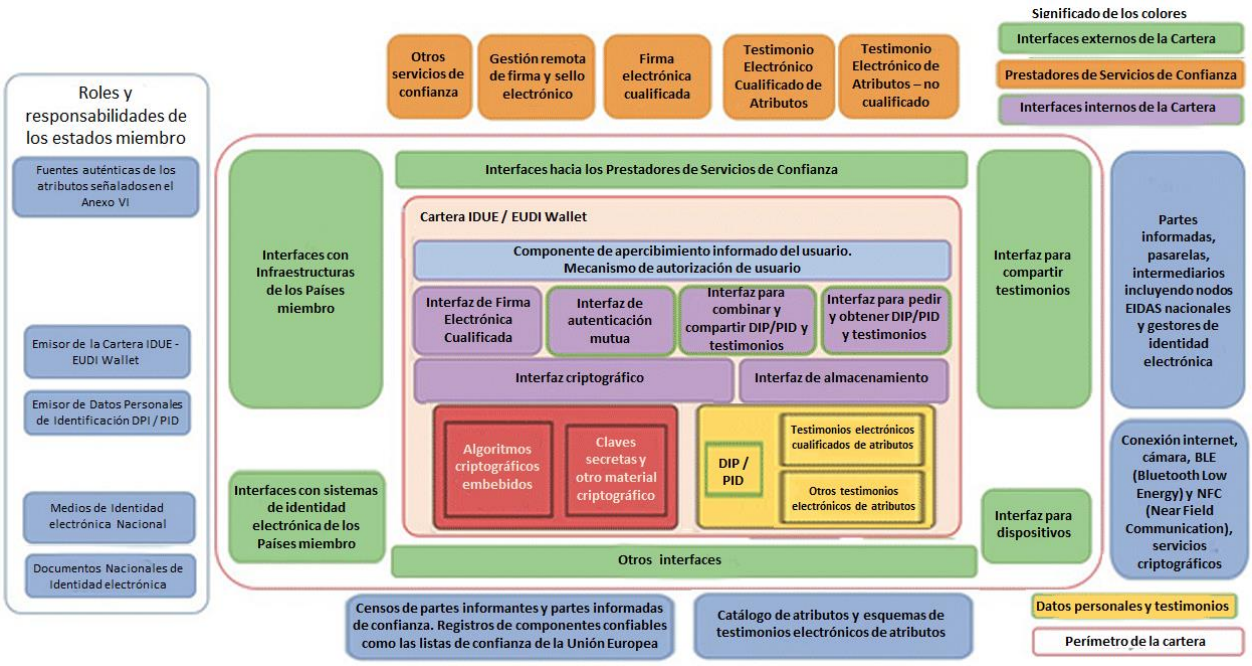


Figura 3 Interfaces de La Cartera IDUE

4.8.1 Interfaz con las infraestructuras de los Estados miembros

Las infraestructuras existentes involucradas en los procesos descritos anteriormente incluyen:

- fuentes auténticas de atributos bajo la responsabilidad de los Estados miembros de conformidad con el Reglamento eIDAS;
- infraestructura de emisión de Cartera IDUE ;
- infraestructura de prueba de identidad asociada a la emisión de la Cartera IDUE ;
- partes informadas, pasarelas, intermediarios, incluidos los nodos eIDAS y otros plataformas y puertas de enlace nacionales de eID;
- medios de identidad electrónica notificados por los estados miembros en virtud de la normativa EIDAS (Reglamento UE 910/2014).

Varios procesos y entidades están bajo la responsabilidad de los Estados miembros y, como tales, se **establecerán** interfaces entre la cartera EUDI y las infraestructuras correspondientes de los Estados miembros para gestionar, en particular:

- la verificación de identidad aplicando procedimientos de alto nivel de aseguramiento durante el proceso de inscripción;
- la emisión la Cartera EUDI con los datos DIP/PID del usuario durante el proceso de inscripción;
- la aportación de datos DIP/PID del usuario partiendo de fuentes auténticas de información de atributos;
- el despliegue, en términos generales, de conectividad adecuada entre las infraestructuras de identidad electrónica existentes y la cartera EUDI para autenticar a su titular.

4.8.2 Interfaz con los documentos nacionales de identidad de los Estados miembros

De conformidad con el Reglamento 2019/1157[26], los documentos de identidad de los Estados miembros contienen DIP/PID testimoniados en formato digital, accesibles a través de interfaces sin contacto. La Cartera IDUE **puede** aprovechar estos datos en sus flujos de trabajo, por ejemplo, para:

- Obtener DIP/PID testimoniados electrónicamente;
- Dar soporte al proceso de verificación de identidad;
- Reforzar las declaraciones de identidad o de autenticación.

Pueden ser necesarias infraestructuras nacionales además de la interfaz sin contacto con el chip del documento nacional de identidad, por ejemplo, para proporcionar datos DIP/PID sobre la base de los datos contenidos en los carnets de identidad.

Los pasaportes y los documentos nacionales de identidad que **contengan** componentes electrónicos también pueden ser adoptados entre los mecanismos de interfaz.

4.8.3 Interfaz hacia partes informadas, pasarelas o intermediarios[27]

Algunas partes informadas **pueden** considerarse como intermediarios que actúan como representantes de otros terceros entre la Cartera IDUE y los testimoniadores electrónicos de atributos o que facilitan el soporte al protocolo de intercambio de datos DIP/PID y otros protocolos de identificación y autenticación. Cuando una parte informada actúa como representante de otra parte informada, la fiabilidad del mecanismo de autenticación **no debe** verse afectada. El presente documento no distingue entre las partes informadas que se conectan por sí mismas o las que lo hacen a través de otros intermediarios. Ambos se consideran partes informadas a las que se aplican los mismos requisitos técnicos.

El protocolo de acceso a testimonios procedentes de partes informantes **puede** unificarse con el protocolo de identificación y autenticación de los medios de identidad electrónica de la Cartera IDUE por razones de simplicidad, facilidad de adopción, seguridad y mantenibilidad.

4.8.4 Interfaces con registros de entidades confiables

La Cartera IDUE interactúa con un ecosistema complejo en el que los *censos* de intervinientes confiables son cruciales. Los registros de confianza que representan tales *censos* **deberán** proporcionar a la cartera EUDI y a su usuario la información relativa a la confiabilidad de: [28]

[26] Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo al refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a los ciudadanos de la Unión ay los miembros de su familia que ejerzan su derecho a la libre circulación (DO L 188 de 12.7.2019, p. 67).

[27] En inglés **'proxy/broker/gateway'**. La referencia a pasarelas o intermediarios se utiliza para denotar un papel de intermediario entre un Cartera IDUE y un proveedor de servicios en una infraestructura digital. Los prestadores de servicios pueden introducir un proxy/broker/gateway que implemente la interfaz EUDI Wallet para el proveedor de servicios y, por lo tanto, actúe como parte de confianza para la EUDI Wallet.

[28] Las habilitaciones para los actos de ejecución se proponen en COM(2021)281 final, art. 6 b, apartado 4, artículo 6 b, apartado 6, artículo 6 d, apartado 3.

- prestadores de servicios electrónicos de confianza, recogidos en las listas de confianza de la UE (TLS), las fuentes de información confiables de DIP/PID, las partes informantes sectoriales no cualificadas, las partes informadas de confianza, la lista de carteras EUDI certificadas, etc.;
- Estado de validez de datos contenidos en las carteras EUDI, tales como DIP/PID, TEA/EAA y TECA/QEAA y, compuesto por:
  - el estado de validez de una cartera EUDI individual en particular,
  - la validez de un DIP/PID, TEA/EAA o TECA/QEAA que el prestador o el usuario pueden optar por revocar o suspender en un momento dado.

4.8.5 Interfaces de dispositivos

La Cartera EUDI estará compuesto por uno o varios componentes de software y hardware. Además de los componentes CSP (Cryptography Services Provider), que **pueden** proporcionar servicios de criptografía y capacidades de almacenamiento (como SE – SecureElement–, SIM – Subscriber Identity Module – o soluciones de software evaluadas adecuadamente), otros componentes de hardware en los que se ejecuta el software de la Cartera IDUE **pueden** ser externos a la Cartera IDUE y accesibles a través de interfaces estandarizadas.

Una lista no exhaustiva de esas interfaces incluye:

- Acceso a la red de Internet en línea (a través de una red celular de banda ancha, Wi-Fi o conexión de red de área local – LAN –);
- Sensores, como cámaras de teléfonos inteligentes, sensores IR – Infrarrojos, micrófonos, etc.;
- Canales de comunicación fuera de línea (como BLE – Bluetooth low energy –, Wi-Fi Aware, NFC – Near Fiedl Communications –, etc.); Emisores como pantallas, linternas, altavoces, etc.

5 REQUISITOS NO FUNCIONALES DE LA CARTERA IDUE

En este capítulo se describen las principales limitaciones dentro de las cuales podrán operar las funcionalidades de la Cartera IDUE. Identifica los requisitos obligatorios no funcionales ("**shall**") a raíz de la propuesta legal europea. Esta descripción posiblemente se actualice y se modifique y las funciones opcionales que pueden ser útiles o deseables (**"pueden"**) se puedan identificar en el curso de la labor del grupo de expertos sobre la caja de herramientas (*toolbox*) que ha dado lugar a la presente versión de este documento.

La cartera IDUE **cumplirá** los requisitos establecidos en el artículo 8 del Reglamento eIDAS en lo que respecta al nivel de aseguramiento alto, en particular en lo que respecta a los requisitos de prueba y verificación de identidad, y a la gestión y autenticación de medios de identificación electrónica, tal como se definen en el Reglamento de Ejecución 2015/1502.[29]

[29] Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) 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.

Tal como se establece en la propuesta legislativa europea, las carteras EUDI **serán** interoperables en toda la Unión Europea y tendrán interfaces orientadas al exterior especificadas por normas técnicas comunes. Ciertos casos de uso **pueden** requerir una mayor interoperabilidad internacional.

La Cartera EUDI **deberá** garantizar el pleno control del usuario sobre sus datos almacenados en su Cartera EUDI individual integrando la seguridad y la privacidad desde el diseño. Por lo tanto, las funciones básicas de la Cartera IDUE, como la identificación, la autenticación, la firma electrónica, el sello electrónico y el intercambio de atributos , no se producirán sin el consentimiento[30] del usuario. No obstante, la suspensión y revocación podrá no requerir el consentimiento del usuario que podrá ser informado de ello.

La cartera EUDI **tendrá** una interfaz y una experiencia de usuario fáciles de usar y tomará en consideración la accesibilidad, la usabilidad y la inclusión.

La Cartera EUDI **deberá** apercibir al usuario respecto a su uso y los datos que maneja y, en particular, permitir que el usuario sepa cuándo y cómo se está utilizando o se ha utilizado su Cartera EUDI, que se le informe de la naturaleza de todas las operaciones realizadas con su cartera EUDI y que se presenten todas esas circunstancias ordenadas a lo largo del tiempo. En este contexto, el usuario también **deberá** recibir notificación de las vulneraciones de control, o será razonablemente capaz de detectar vulneraciones de control. La implementación de esta capacidad requerirá un mayor debate para preservar la privacidad del usuario. También será necesario seguir considerando enfoques alternativos para la recuperación del contenido y del material criptográfico de la Cartera por parte del usuario.

La Cartera EUDI **deberá** permitir al usuario compartir únicamente la información que se proponga compartir. La Billetera **deberá** garantizar un nivel adecuado de privacidad, implementando políticas sobre no trazabilidad y *desvinculabilidad* de las actividades del usuario de cara a terceros, según corresponda, considerando:

- el contexto jurídico aplicable a los prestadores de identidad y a los prestadores de testimonios;
- la necesidad de conservar pruebas electrónicas utilizables en contextos de resolución de litigios;
- el derecho del usuario a ser informado del uso de su cartera EUDI.

Con el fin de brindar confianza a los usuarios de la Cartera IDUE, a las partes informadas y otras partes que confían, el emisor de la Cartera IDUE **deberá** garantizar la conformidad de los componentes críticos de la implementación de la Cartera IDUE (incluidas las funcionalidades principales de la Cartera IDUE y la implementación de protocolos de interfaz). La conformidad deberá ser confirmada por una certificación reconocida de la Cartera IDUE[31]. La seguridad de los componentes críticos integrados en la cartera EUDI o utilizados por la cartera EUDI, que protegen contra el uso indebido o la alteración de los datos de identificación, el mecanismo de autenticación o el mecanismo de consentimiento**,** se certificará de conformidad con la propuesta legal europea. [32]

[30] El "consentimiento" del usuario representa la voluntad informada del usuario de llevar a cabo una operación, como realizar una identificación electrónica, realizar una firma electrónica cualificada, compartir atributos, etc (consentimiento informado).

[31] Artículo 6 c de la norma COM(2021) 281 final.

[32] El artículo 6 c, apartado 1, establece que las carteras europeos de identidad digital que hayan sido certificados o para los que se haya emitido una declaración de conformidad en virtud de un esquema de ciberseguridad de conformidad con el Reglamento (UE) 2019/881 y cuyas referencias se hayan publicado en el Diario Oficial de la Unión Europea se presumirá que cumple los requisitos pertinentes en materia de ciberseguridad establecidos en

Además, el mecanismo para que las partes informadas y otras partes que confían comprueben si una cartera EUDI utilizada es genuina (auténtica) y está certificada no permitirá que la parte que confía distinga entre dos carteras EUDI certificadas, con el fin de preservar la privacidad de su usuario al realizar una autenticación en base a seudónimo. Los prestadores de servicios de confianza **no recibirán** ninguna información sobre el uso dado a los testimonios proporcionados.

El emisor de la Cartera EUDI **no recopilará** información sobre el uso de la Cartera EUDI, que no sea necesaria para la prestación de los servicios de la Cartera EUDI. Además, el emisor de Cartera **no deberá** combinar DIP/PID y cualquier otro dato personal almacenado o relacionado con el uso de la Cartera IDUE con datos personales de cualquier otro servicio ofrecido por este emisor o por prestadores terceros, que no sean necesarios para la prestación de los servicios de la Cartera IDUE, a menos que el usuario lo haya solicitado expresamente. Los datos personales relacionados con el suministro de Carteras Europeas de Identidad Digital se mantendrán física y lógicamente separados de cualquier otro dato almacenado.

6 MÓDULOS POTENCIALES DE LA CARTERA EUDI

La implementación de las funcionalidades de la Cartera IDUE presentadas en el Capítulo 4 de este documento puede ser proporcionada por diferentes tecnologías. Estas tecnologías existentes se pueden segmentar en bloques modulares para identificar el conjunto de componentes, que pueden componer el núcleo de la Cartera IDUE .

Las diferentes funciones de la Cartera IDUE se pueden implementar utilizando tecnologías existentes como:

- Factores de forma
    - Factor de forma 1: Aplicación móvil
    - Factor de forma 2: Aplicación web
    - Factor de forma 3: Aplicación segura en PC
- Bloques funcionales
    - Bloque 1: Servidor back-end que incluye HSM evaluado (Dispositivo Cualificado)
    - Bloque 2: Documentos electrónicos oficiales de identidad
    - Bloque 3: Token externo seguro de hardware
    - Bloque 4: Prestador de servicios criptográficos
    - Bloque 5: Entorno de ejecución de confianza (Trusted execution environment - TEE)

Los factores de forma pueden, además de la interfaz de usuario, proporcionan:

- Autenticación de usuarios para garantizar el consentimiento.
- Almacenamiento (nivel de seguridad dependiendo del módulo utilizado).
- Acceso a dispositivos DCCF/DCCS/QSCD y funcionalidades basadas en la nube (nivel de seguridad dependiendo del módulo utilizado).

---

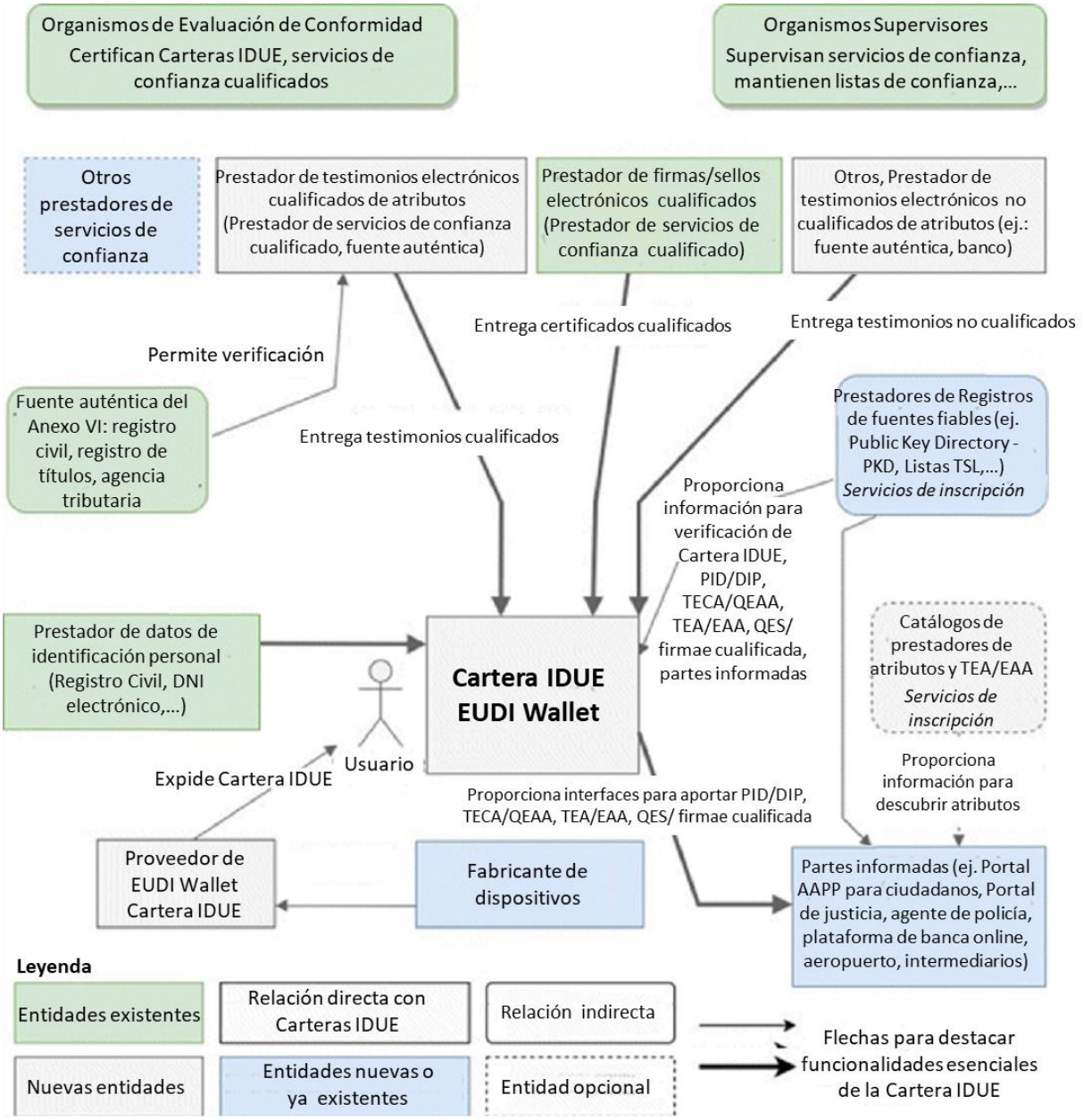
el artículo 6 a, apartados 3, 4 y 5, en la medida en que el certificado o la declaración de conformidad en materia de ciberseguridad o partes del mismo cubrir esos requisitos.

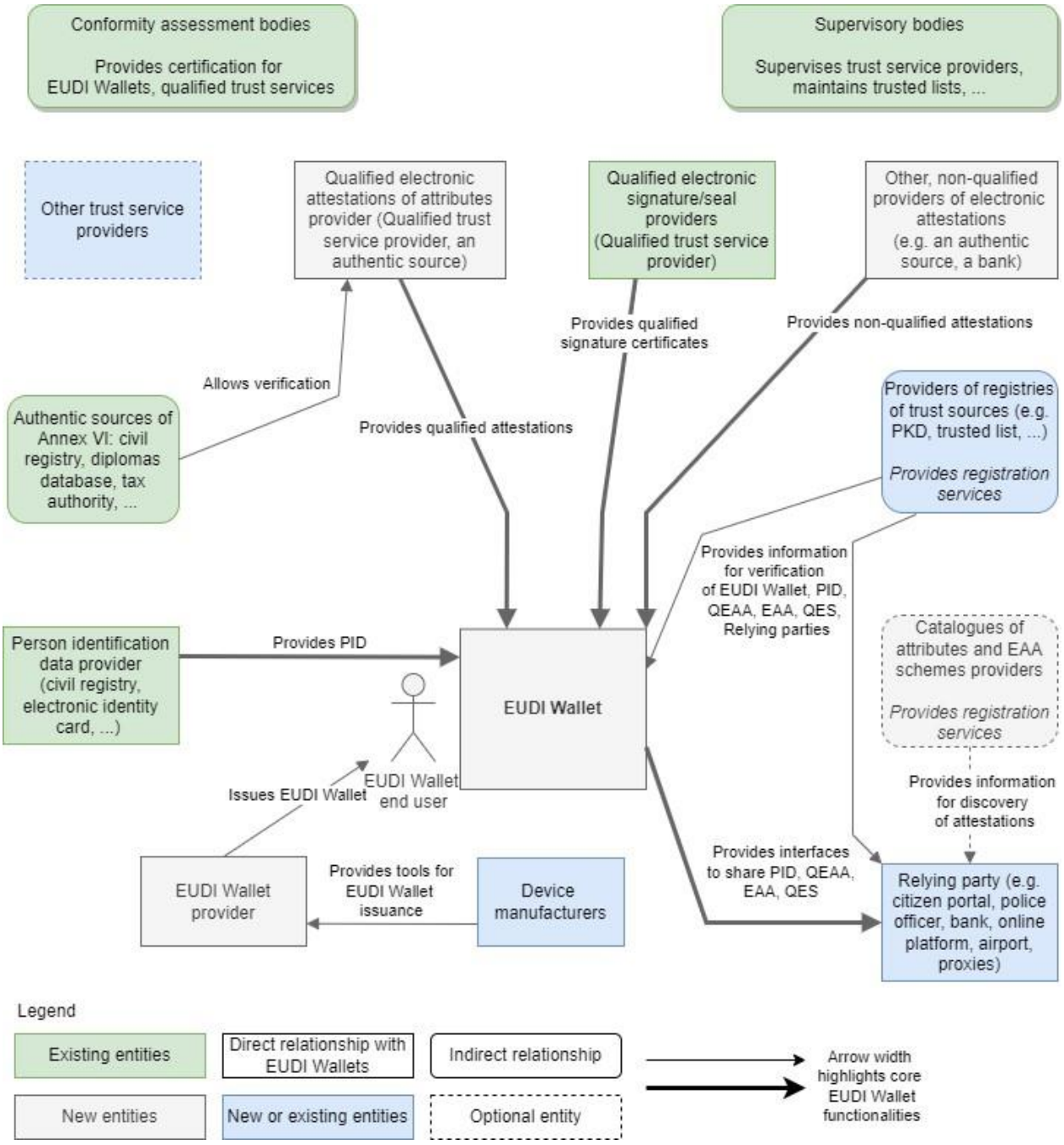
Los bloques funcionales, dependiendo de la implementación, pueden, junto con el factor de forma, proporcionar:

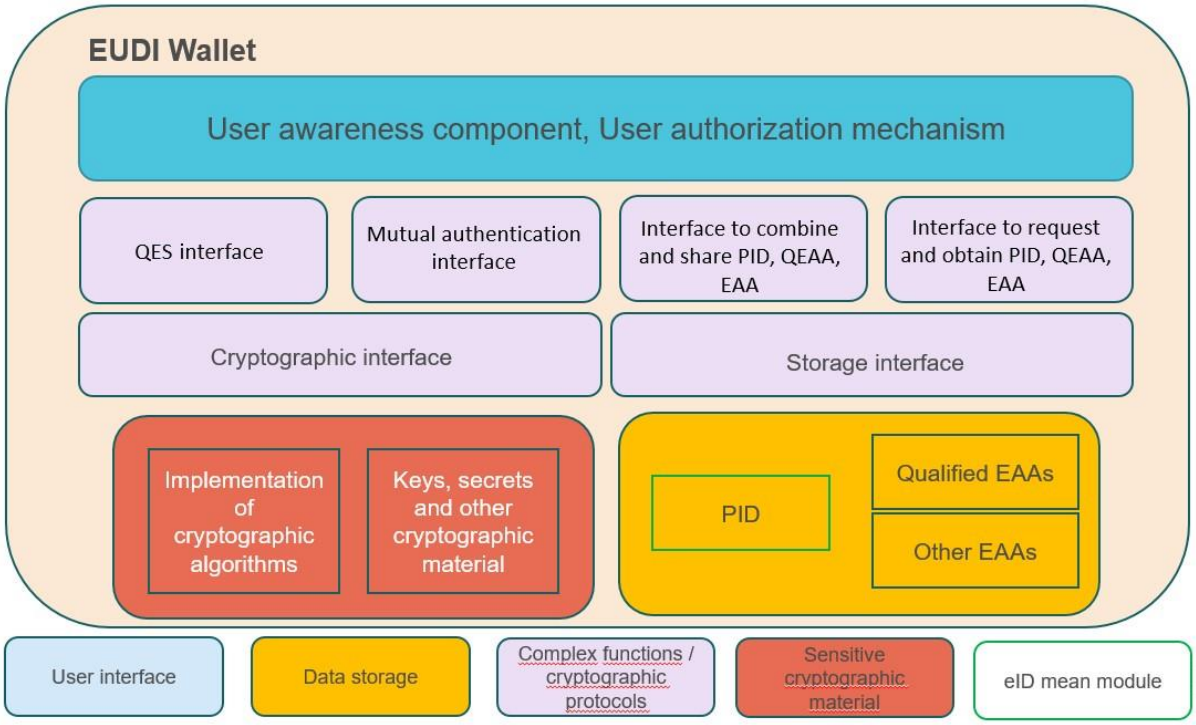
- Almacenamiento seguro en el módulo (con limitaciones);
- Autenticación fuerte de usuario;
- Almacenamiento seguro y cifrado;
- Autenticación mutua;
- Firmas electrónicas cualificadas;
- Acceso seguro a servicios en la nube.

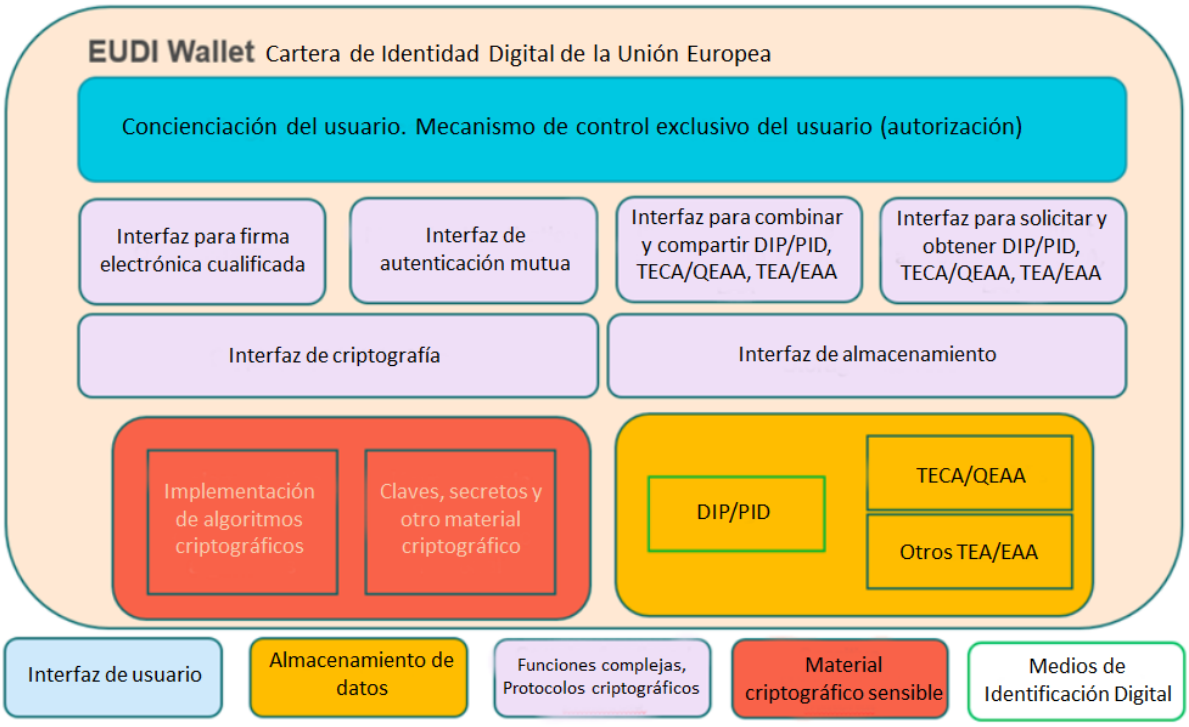
Diagramas en inglés y en español

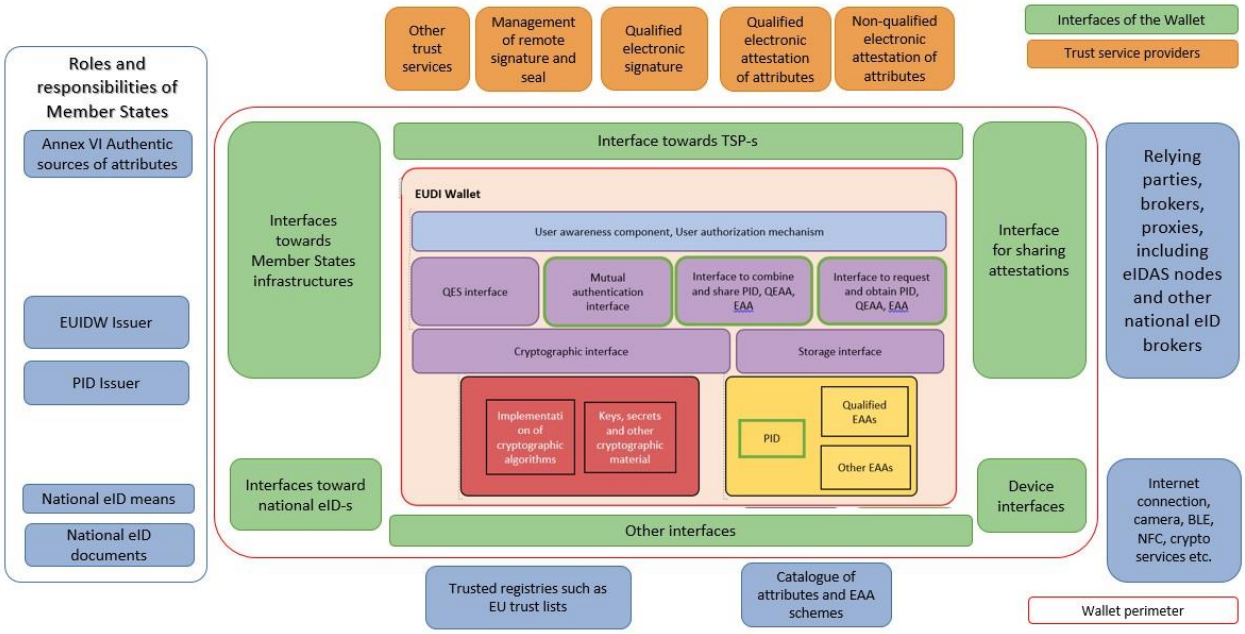
Para comparar las traducciones adoptadas

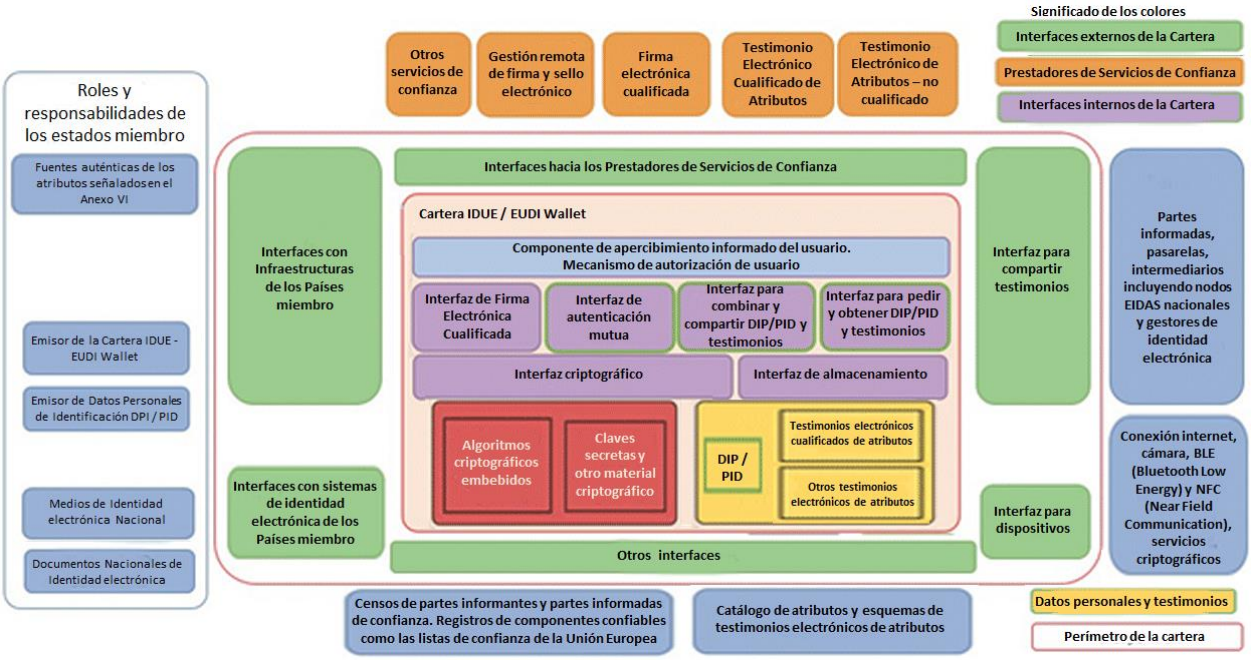



Conformity assessment bodies
Provides certification for EUDI Wallets, qualified trust services
Supervisory bodies
Supervises trust service providers, maintains trusted lists, ...
Other trust service providers
Qualified electronic attestations of attributes provider (Qualified trust service provider, an authentic source)
Qualified electronic signature/seal providers (Qualified trust service provider)
Other, non-qualified providers of electronic attestations (e.g. an authentic source, a bank)
Allows verification
Provides qualified signature certificates
Provides non-qualified attestations
Authentic sources of Annex VI: civil registry, diplomas database, tax authority, ...
Provides qualified attestations
Providers of registries of trust sources (e.g. PKD, trusted list, ...)
Provides registration services
Provides information for verification of EUDI Wallet, PID, QEAA, EAA, QES, Relying parties
Person identification data provider (civil registry, electronic identity card, ...)
Provides PID
EUDI Wallet
Catalogues of attributes and EAA schemes providers
Provides registration services
Issues EUDI Wallet
EUDI Wallet end user
Provides information for discovery of attestations
Provides interfaces to share PID, QEAA, EAA, QES
EUDI Wallet provider
Provides tools for EUDI Wallet issuance
Device manufacturers
Relying party (e.g. citizen portal, police officer, bank, online platform, airport, proxies)
Legend
Existing entities
Direct relationship with EUDI Wallets
Indirect relationship
Arrow width highlights core EUDI Wallet functionalities
New entities
New or existing entities
Optional entity


EUDI Wallet
User awareness component, User authorization mechanism
QES interface
Mutual authentication interface
Interface to combine and share PID, QEAA, EAA
Interface to request and obtain PID, QEAA, EAA
Cryptographic interface
Storage interface
Implementation of cryptographic algorithms
Keys, secrets and other cryptographic material
PID
Qualified EAAs
Other EAAs
User interface
Data storage
Complex functions / cryptographic protocols
Sensitive cryptographic material
eID mean module


EUDI Wallet Cartera de Identidad Digital de la Unión Europea
Concienciación del usuario. Mecanismo de control exclusivo del usuario (autorización)
Interfaz para firma electrónica cualificada
Interfaz de autenticación mutua
Interfaz para combinar y compartir DIP/PID, TECA/QEAA, TEA/EAA
Interfaz para solicitar y obtener DIP/PID, TECA/QEAA, TEA/EAA
Interfaz de criptografía
Interfaz de almacenamiento
Implementación de algoritmos criptográficos
Claves, secretos y otro material criptográfico
DIP/PID
TECA/QEAA
Otros TEA/EAA
Interfaz de usuario
Almacenamiento de datos
Funciones complejas, Protocolos criptográficos
Material criptográfico sensible
Medios de Identificación Digital


Roles and responsibilities of Member States
Annex VI Authentic sources of attributes
EUIDW Issuer
PID Issuer
National eID means
National eID documents
Other trust services
Management of remote signature and seal
Qualified electronic signature
Qualified electronic attestation of attributes
Non-qualified electronic attestation of attributes
Interfaces of the Wallet
Trust service providers
Interfaces towards Member States infrastructures
Interface towards TSP-s
EUDI Wallet
User awareness component, User authorization mechanism
QES interface
Mutual authentication interface
Interface to combine and share PID, QEAA, EAA
Interface to request and obtain PID, QEAA, EAA
Cryptographic interface
Storage interface
Implementation of cryptographic algorithms
Keys, secrets and other cryptographic material
PID
Qualified EAAs
Other EAAs
Interface for sharing attestations
Relying parties, brokers, proxies, including eIDAS nodes and other national eID brokers
Interfaces toward national eID-s
Other interfaces
Device interfaces
Internet connection, camera, BLE, NFC, crypto services etc.
Trusted registries such as EU trust lists
Catalogue of attributes and EAA schemes
Wallet perimeter


Roles y responsabilidades de los estados miembro
Fuentes auténticas de los atributos señaladosen el Anexo VI
Emisor de la Cartera IDUE - EUDI Wallet
Emisor de Datos Personales de Identificación DPI / PID
Medios de Identidad electrónica Nacional
Documentos Nacionales de Identidad electrónica
Otros servicios de confianza
Gestión remota de firma y sello electrónico
Firma electrónica cualificada
Testimonio Electrónico Cualificado de Atributos
Testimonio Electrónico de Atributos – no cualificado
Significado de los colores
Interfaces externos de la Cartera
Prestadores de Servicios de Confianza
Interfaces internos de la Cartera
Interfaces con Infraestructuras de los Países miembro
Interfaces hacia los Prestadores de Servicios de Confianza
Cartera IDUE / EUDI Wallet
Componente de apercibimiento informado del usuario. Mecanismo de autorización de usuario
Interfaz de Firma Electrónica Cualificada
Interfaz de autenticación mutua
Interfaz para combinar y compartir DIP/PID y testimonios
Interfaz para pedir y obtener DIP/PID y testimonios
Interfaz criptográfico
Interfaz de almacenamiento
Algoritmos criptográficos embebidos
Claves secretas y otro material criptográfico
DIP / PID
Testimonios electrónicos cualificados de atributos
Otros testimonios electrónicos de atributos
Interfaz para compartir testimonios
Partes informadas, pasarelas, intermediarios incluyendo nodos EIDAS nacionales y gestores de identidad electrónica
Interfaces con sistemas de identidad electrónica de los Países miembro
Otros interfaces
Interfaz para dispositivos
Conexión internet, cámara, BLE (Bluetooth Low Energy) y NFC (Near Field Communication), servicios criptográficos
Censos de partes informantes y partes informadas de confianza. Registros de componentes confiables como las listas de confianza de la Unión Europea
Catálogo de atributos y esquemas de testimonios electrónicos de atributos
Datos personales y testimonios
Perímetro de la cartera

Documentación complementaria.

Esta documentación no formaba parte del documento original

ANEXO
de la propuesta de
Reglamento del Parlamento Europeo y del Consejo
por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea
{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

ANEXO I
En el anexo I, el punto i) se sustituye por el siguiente texto:

«i) la información o la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;».

ANEXO II

REQUISITOS DE LOS DISPOSITIVOS CUALIFICADOS DE CREACIÓN DE FIRMA ELECTRÓNICA

1. Los dispositivos cualificados de creación de firma electrónica garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

   a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas;
   b) los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas solo puedan aparecer una vez en la práctica;
   c) exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas no pueden ser hallados por deducción y de que la firma electrónica está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento;
   d) los datos de creación de la firma electrónica utilizados para la creación de firmas electrónicas puedan ser protegidos con seguridad por el firmante legítimo contra su utilización por otros.

2. Los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.

ANEXO III
En el anexo III, el punto i) se sustituye por el texto siguiente:

«i) la información o la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;».

ANEXO IV
En el anexo IV, el punto j) se sustituye por el texto siguiente:

«j) la información o la localización de los servicios de estado de validez del certificado que pueden utilizarse para consultar el estado de validez del certificado cualificado.».

ANEXO V

REQUISITOS DE LA DECLARACIÓN ELECTRÓNICA CUALIFICADA DE ATRIBUTOS

La declaración electrónica de atributos cualificada contendrá:

a) una indicación, al menos en un formato adecuado para el tratamiento automático, de que la declaración ha sido expedida como declaración electrónica de atributos cualificada;
b) un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide la declaración electrónica de atributos cualificada, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y
   - para las personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,
   - para las personas físicas: el nombre de la persona,
c) un conjunto de datos que represente inequívocamente a la entidad a que se refieren los atributos declarados; si se usara un seudónimo, se indicará claramente;
d) el atributo o atributos declarados, incluyendo, cuando proceda, la información necesaria para identificar el alcance de dichos atributos;
e) los datos relativos al inicio y final del período de validez de la declaración;
f) el código de identidad de la declaración, que debe ser único para el prestador cualificado de servicios de confianza y, si procede, la indicación del régimen de declaraciones al que pertenece la declaración de atributos;
g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;
h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra f);
i) la información o la localización de los servicios que pueden utilizarse para consultar el estado de validez de la declaración cualificada.

ANEXO VI

LISTA MÍNIMA DE ATRIBUTOS

Además de lo dispuesto en el artículo 45 quinquies, los Estados miembros garantizarán la adopción de medidas que permitan a los prestadores cualificados de declaraciones electrónicas de atributos verificar por medios electrónicos, a petición del usuario, la autenticidad de los atributos siguientes, cotejándolos con las fuentes auténticas pertinentes a escala nacional o a través de intermediarios designados reconocidos a escala nacional, de conformidad con el Derecho nacional o de la Unión y en los casos en que tales atributos se basen en fuentes auténticas pertenecientes al sector público:

1. dirección,
2. edad,
3. sexo,
4. estado civil,
5. composición familiar,
6. nacionalidad,
7. cualificaciones, títulos y licencias académicos,
8. cualificaciones, títulos y licencias profesionales,

9. permisos y licencias públicos,
10. datos financieros y sociales.