A Caixa de xeramentas Común da Unión para un enfoque coordinado cara a un Marco Europeo de Identidade Dixital

Arquitectura e marco de referencia da carteira europea de identidade dixital

Abril de 2023

Versión 1.1.0

VERSIÓN DO DOCUMENTO

VERSIÓN	DATA[1]	CAMBIOS
1.0.0	26 de xaneiro de 2023	Primeira versión
1.1.0	20 de abril de 2023	Adición de planos de servicios para casos de uso en: - Identificación e autenticación para acceder aos servizos en liña, e - permiso de condución móbil

[1] A data de adopción polo Grupo de Expertos eIDAS

Contido

1. Introdución

1.1. Contexto

O 3 de xuño de 2021, a Comisión Europea adoptou unha Recomendación[2] en que se pide aos Estados membros que traballen no desenvolvemento dunha caixa de ferramentas que inclúa unha arquitectura técnica e un marco de referencia (no sucesivo, o ARF, pola súa designación en inglés "Arquitecture and Reference Framework"), un conxunto de normas comúns e especificacións técnicas e un conxunto de directrices comúns e mellores prácticas.

A Recomendación especifica que estes resultados servirán de base para a aplicación da proposta de Marco Europeo de Identidade Dixital sen [3] que o proceso de elaboración da caixa de pechamentas interfira ou prexulgue o proceso lexislativo.

A Recomendación prevé que a caixa de xeramentas sexa desenvolvida por expertos dos Estados membros no Grupo de Expertos eIDAS[4]en estreita coordinación coa Comisión e, cando sexa pertinente para o funcionamento da infraestrutura da Carteira de Identidade Dixital da Unión Europea (IDUE), con outras partes interesadas dos sectores público e privado.

Seguindo o calendario indicativo establecido na Recomendación, o 30 de setembro de 2021 acordáronse un proceso e uns procedementos de traballo que se debateron nun documento oficioso sobre unha descrición de alto nivel do ecosistema Carteira IDUE, proposto pola Comisión.

Sobre esta base, entre outubro e decembro de 2021 definiuse un esquema que proporcionaba unha descrición máis detallada do concepto de carteira IDUE, as súas funcionalidades e aspectos de seguridade, así como de varios casos de uso básicos. Ese traballo deu lugar ao Esbozo do ARF, adoptado polo Grupo de Expertos eIDAS en febreiro de 2022. O esquema publicouse en Futurium[5] para trasladar a opinión do público. Cando se pechou o decreto de comentarios o 15 de abril de 2022, 36 partes interesadas enviaran os seus comentarios sobre o Esbozo.

Desde entón, o Grupo de Expertos eIDAS seguiu desenvolvendo os conceptos e especificacións do Marco Europeo de Identidade Dixital sobre a base da proposta de revisión do Regulamento

[2] RECOMENDACIÓN DA COMISIÓN (UE) C(2021) 3968 final do 3 de xuño de 2021 sobre unha caixa de forramentas común da Unión para un enfoque coordinado cara a un marco europeo de identidade dixital, DO L 210/51 de 14.6.2021.

[3] Todas as referencias no documento á revisión do Regulamento eIDAS débense entender feitas á proposta da Comisión do 3 de xuño de 2021, salvo indicación en contrario. Proposta de REGULAMENTO DO PARLAMENTO EUROPEO E DO CONSELLO POLO que se modifica o Regulamento (UE) nº 910/2014 no que respecta ao establecemento dun marco para a identidade dixital 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

EIDAS da Comisión[6] e seguirá facéndoo ata que conclúan as negociacións lexislativas e se adopten os actos de execución.

O Grupo de Expertos eIDAS adoptou este documento o 20 de abril de 2023.

1.2. Sobre este documento

1.2.1. Autoría e licencia

Este documento é o resultado do traballo do Grupo de Expertos eIDAS (eIDAS Expert Group) (E03032)[7] cuxa última reunión tivo lugar o 20/03/2023 (para os efectos desta versión do documento).

A versión orixinal en inglés deste documento mantida nunha ferramenta que promove a cooperación e contribucións de diferentes autores está dispoñible en https://code.europa.eu/eudi/architecture-and-reference-framework

Esta forma de xestionar o documento fai recomendable recorrer a esa URL para acceder ás versións máis actualizadas do documento en inglés.

1.2.2. Traducción e licencia.

A versión en español a realizou **Julián Inza**, Presidente de EADTRUST, un Prestador Cualificado de Servizos de Confianza radicado en Madrid (España) con páxina web https://eadtrust.eu e finalizouse o 11 de setembro de 2023, varias semanas días despois de que se publicase a versión

[6] Todas as referencias do documento á revisión do Regulamento eIDAS débense entender feitas á proposta da Comisión do 3 de xuño de 2021, salvo que se indique o contrario.
[7] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3032

orixinal en inglés na páxina web de Github https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

Calquera obra derivada debe indicar que se desenvolveu a partir da tradución realizada por **Julián Inza**, Presidente de EADTRUST European Agency of Dixital Trust, S.L, un Prestador Cualificado de Servizos de Confianza radicado en Madrid (España) con páxina web https://eadtrust.eu

1.2.3. Finalidade deste documento.

O obxectivo do documento é proporcionar todas as especificacións necesarias para desenvolver unha solución interoperable de carteira IDUE basada en normas e prácticas comúns. O documento presenta un estado dos traballos en curso do Grupo de Expertos eIDAS e non implica ningún acordo formal sobre o seu contido ou a proposta de revisión do Regulamento eidas. Este documento complementarase e actualizarase co tempo a través do proceso de creación da caixa de xeramentas, tal e como se describe no capítulo 8. Unha vez completado, o documento describirá unha Arquitectura e un Marco de Referencia completos que abranguerán todas as especificacións necesarias para implantar unha Solución Europea de Carteira de Identidade Dixital.

Mentres que os capítulos 2-4 e 7-8 son descritivos, os capítulos 5 e 6 especifican os requisitos para os prestadores de DEP/PID e TE(C)A/(Q)EAA e os implementadores de solucións de Carteira IDUE. As expresións imperativas en maiúsculas no documento utilízanse de acordo coa norma técnica RFC 2119.

O documento en si non ten valor legal e non prexulgará o proceso lexislativo en curso e os requisitos legais obrigatorios finais para as carteiras europeas de identidade dixital. O ARF axustarase ao resultado das negociacións lexislativas da proposta de marco europeo de identidade dixital. Só serán obrigatorios o Regulamento marco europeo de identidade dixital finalmente adoptado e os actos de execución e delegados adoptados de acordo coa dita base xurídica.

1.3. Uso deste documento

Este documento está destinado principalmente a ser utilizado pola Comisión Europea que desenvolve unha implementación de referencia dunha Carteira IDUE e os consorcios que executan proxectos piloto enfocados no uso da implementación de referencia no contexto de "Lonxe Scale Pilots" (Pilotos a Gran Escala). A experiencia adquirida na aplicación desta especificación pode dar lugar a melloras deste documento, de conformidade co capítulo 8.

1.3.1. A implementación de referencia dunha carteira IDUE

A Comisión proporcionará unha implementación de referencia da carteira IDUE nun formato móbil[8]. O código da implementación de referencia de Carteira IDUE proporcionarase como software de fontes abertas para a súa reutilización polos implementadores de toda europa. Os primeiros implementadores serán os proxectos seleccionados para levar a cabo os Lonxe Scale Pilots (LSPs), tras unha convocatoria de propostas semellante a unha licitación. Os proxectos LSP participarán no desenvolvemento da implementación de referencia dunha Carteira IDUE. A Comisión tamén prestará inicialmente os servizos centrais necesarios para o funcionamento da implementación de referencia da Carteira IDUE.

A Comisión proponse utilizar o ARF para desenvolver a aplicación de referencia da Carteira IDUE.

1.3.2. Orientacións para os pilotos a gran escala (Lonxe Scale Pilots LSP)

Para apoiar o desenvolvemento dunha implementación de referencia dunha carteira IDUE e probar o seu uso a través de diferentes casos de uso prioritarios en proxectos piloto, a Comisión lanzou unha convocatoria de propostas o 22 de febreiro de 2022 no marco do Programa Europa Dixital para acoller casos de uso a gran escala para a carteira IDUE.

O obxectivo da convocatoria Lonxe Scale Pilots (LSP) é cofinanciar proxectos piloto que fagan uso da carteira IDUE superada nunha implementación de referencia do software de carteira IDUE, tendo en conta as especificidades do proxecto, os sistemas existentes de Identidade Dixital notificados (como o DNIe no caso de España) e os desenvolvementos nacionais de sistemas de carteira e as situacións de implementación, arredor dos diferentes casos de uso transfronteirizos que implican a partes interesadas tanto públicas como privadas.

O ARF será utilizado polos LSP para informar e guia-lo deseño de sistemas dos pilotos e o desenvolvemento da arquitectura xunto coa publicación da implementación de referencia.

Espérase que os LSP acheguen os seus comentarios sobre o ARF a medida que desenvolvan e interactúen cos servizos das partes de confianza, os provedores cualificados ou non cualificados de testemuños electrónicos de atributos TE(C)A/(Q)EAA, os provedores de datos de identificación de persoas (DIP/PID) e os usuarios en transaccións significativas segundo os casos de uso propostos.

[8] Actualmente está prevista unha primeira versión para o segundo trimestre de 2023, á que seguirán outras.

2. Definicións

Ademais do artigo 3 da proposta de modificación do texto legal do Regulamento eIDAS (anterior regulamento UE 910/2014) ofrécense as seguintes definicións para destacar as máis relevantes para a Arquitectura e o Marco de Referencia ou para introducir termos adicionais non definidos no citado texto legal (sinalados cun *).

Atributo	**Rasgo, característica ou calidade dunha persoa física ou xurídica ou dunha entidade, en forma electrónica. - *Proposta de modificación do Regulamento eIDAS***
Fonte auténtica	**Repositorio ou sistema, mantido baixo a responsabilidade dun organismo do sector público ou unha entidade privada, que contén atributos sobre unha persoa física ou xurídica e considérase a fonte primaria desa información ou se recoñece como auténtica na lexislación nacional. - *Proposta de modificación do Regulamento eIDAS***
Testemuño electrónico de atributos (TEA)	*En inglés: Electronic Attestation of Attributes (EAA)* **Un testemuño en formato electrónico que permite a autenticación de atributos - *Proposta de modificación do Regulamento eIDAS***
*Emisor**	**Un prestador que informa sobre datos de identificación de persoa (DIP/PID) ou un prestador de servicios de confianza (cualificado ou no) que emite atributos TE(C)A/(Q)EAA. No caso da carteira IDUE, pode haber varios emisores de DIP/PID e de TE(C)A/(Q)EAA.**
Organismos nacionais de acreditación (ONA).*	*En inglés: National Accreditation Bodies (NAB)* **Os Organismos Nacionais de Acreditación (ONA) de acordo co Regulamento (CE) nº 765/2008 son os organismos dos Estados membros que realizan a acreditación de organismos de avaliación de conformaidade con autoridade derivada do Estado.**
Datos de identificación da persoa (DIP)	*En inglés: Person Identification Data (PID)* **Conxunto de datos que permiten establecer a identidade dunha persoa física ou xurídica, ou dunha persoa física que representa a unha persoa xurídica - *Regulamento eIDAS*.**
*Provedor de datos de identificación de persoas**	**Estado membro ou entidade xurídica que proporciona datos de identificación da persoa aos usuarios como fonte primaria.**

Infraestructura de clave pública (PKI).*	*En inglés, Public Key Infraestructure (PKI)* **Denota sistemas, software e protocolos de comunicación que utilizan os compoñentes dunha Carteira IDUE para distribuír, xestionar e controlar claves públicas. Unha PKI entrega claves públicas embebidas en certificados e xestiona a súa confiabilidade respondendo sobre a vixencia dos certificados que emitiu.**
Prestador de Testemuños electrónicos cualificadas de atributos	**Provedor cualificado de servicios de confianza que expide testemuños electrónicos de atributos, e que cumpre os requisitos establecidos no anexo V. - *Proposta de modificación do Regulamento eIDAS***
Dispositivo Cualificado de Creación de Firma (DCCF)	*En inglés, Qualified Signature creation Device (QSCD)* **Software ou hardware configurado para crear asinas electrónicas que cumpra os requisitos establecidos no anexo II da proposta de modificación do Regulamento eIDAS. *Regulamento eIDAS e proposta de modificación do Regulamento eIDAS***
Prestador cualificado de servicios de confianza (PCSC)	*En inglés, Qualified Trust Service Provider (PCSC)* **Un provedor de servicios de confianza que presta un ou varios servicios de confianza cualificados cando o organismo de supervisión lle concedese a condición de cualificase. - *Regulamento eIDAS***
Parte que confía Parte informada*	**Persoa física ou xurídica que confía nunha identificación electrónica ou nun servicio de confianza. - *Regulamento eIDAS*** **No caso de Carteira IDUE, a parte que recibe a información de identificación electrónica ou de atributos procedente de Carteira IDUE.**
Divulgación selectiva.*	**Capacidade da carteira IDUE que permite ao usuario presentar un subconxunto de atributos de entre os que figuran nos DEP/PID ou nos TE(C)A/(Q)EAA.**
*Confianza**	**A confianza é a característica pola que unha parte está disposta a confiar nunha terceira entidade para que execute unha serie de accións e/ou realice unha serie de afirmacións sobre unha serie de temas e/ou ámbitos.[9].**
*Marco de confianza**	**Conxunto xuridicamente esixible de normas e acordos operativos e técnicos que rexen un sistema de múltiples intervenientes deseñado para realizar determinados tipos de transaccións entre unha comunidade de participantes e suxeito a un conxunto común de requisitos.**

[9] Segundo especificacións de "OASIS Trust", [en liña]. Dispoñible: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html.

*Modelo de confianza **	**Conxunto de normas que garanten a lexitimidade dos compoñentes e as entidades que interveñen no ecosistema da carteira IDUE.**
Provedor de servizos de confianza (PSC)	*En inglés, Trust Service Provider (TSP)* **Persoa física ou xurídica que presta un ou varios servicios de confianza, xa sexa como prestador de servicios de confianza cualificado ou como prestador de servicios de confianza non cualificado. - *Regulamento eIDAS***
Servicio de confianza	**Un servicio electrónico prestado normalmente logo de pagamento que consiste en:** **(a) a creación, verificación e validación de certificados electrónicos que respaldan sinaturas electrónicas e selos electrónicos, a emisión de selos de tempo electrónicos, a prestación de servicios de entrega electrónica certificada e a prestación de servicios de testemuño electrónico de atributos;** **(b) a creación, verificación e validación de certificados para a autenticación de sitios web;** **(c) a conservación de documentos electrónicos que inclúen sinaturas electrónicas ou selos electrónicos;** **(d) o arquivo electrónico de documentos electrónicos;** **(e) a xestión de dispositivos remotos de creación de sinaturas e selos electrónicos, baixo control do seu titular, securizando o emprego de claves privadas e certificados;** **(f) o rexistro de datos electrónicos nun libro diario de movementos semellante a un rexistro de contabilidade electrónico. -** ***Proposta de modificación do Regulamento eIDAS***
*Lista de confianza**	**Repositorio de información sobre entidades dotadas de autoridade nun determinado contexto legal ou contractual que proporciona información sobre o seu estado actual e histórico. As listas de confianza poden implementarse de diferentes maneiras.**
*Usuario**	**É unha persoa física ou xurídica que utiliza unha Carteira IDUE.**
*Instancia de carteira IDUE**	**Instancia dunha solución de Carteira IDUE pertencente a un usuario e que está baixo o seu control.**
*Provedores de carteiras IDUE**	**Organización, pública ou privada, responsable do funcionamento dunha solución de carteira IDUE compatible con eIDAS que se pode instanciar, por exemplo, mediante a súa instalación e inicialización.**

Solución Cartera IDUE.*	**Unha solución de carteira IDUE é o conxunto de productos e servicios completo propiedade dun provedor de carteiras IDUE, ofrecido a tódolos usuarios da dita solución. Unha solución Carteira IDUE pode ser certificada como conforme con IDUE por un CAB.**

Cadro 1. Definicións

** Adicional ás definicións do artigo 3 do Regulamento eIDAS ou a súa proposta de modificación.*

3. Casos de uso da carteira EUDI

O desenvolvemento das especificacións de Carteira IDUE (EUDI Wallet) réxese por casos de uso que facilitan a comprensión da experiencia do usuario á vez que captan a proposta de valor e os requisitos empresariais da Carteira IDUE. Para iso, o Grupo de Expertos de eIDAS comeza creando modelos de servizo para cada caso de uso da Carteira IDUE. Estes esquemas son representacións visuais dos distintos compoñentes e procesos que interveñen na prestación dun servicio ós usuarios e serven como ferramenta para identificar posibles áreas de mellora, optimiza-la experiencia do usuario e axiliza-la prestación do servicio. Estes esquemas serven de base para establecer regras de uso e especificacións comúns para todos os casos de uso.

Os esquemas de servicio do caso de uso atópanse nos anexos como documentos adxuntos. É importante sinalar que os esquemas de servicio ofrecen unha solución viable para cada caso de uso, pero existen alternativas e pasos opcionais. Por exemplo, mostrar datos almacenados para os que o usuario xa deu o seu consentimento pode ser opcional. Ademais, os percorridos do usuario (user xourneys) poden variar en función do enfoque de implementación elixido, como o almacenamento asíncrono de atributos ou a recuperación síncrona. Isto podería afectar a aspectos como a prestación do consentimento para recuperar e compartir datos.

O Grupo de Expertos eIDAS describiu esquemas de servizo para os seguintes casos de uso.

3.1 Identificación e autenticación para acceder a servizos en liña

O obxectivo principal da Carteira IDUE é ofrecer unha identificación e autenticación seguras dos usuarios cun alto Nivel de Aseguramento (Level of Assurance, LoA) para os servizos en liña públicos e privados. Esta funcionalidade esencial garante que as partes informadas poidan verificar con seguridade que están interactuando coa persoa correcta.

Neste caso, o usuario utiliza a Carteira IDUE para confirmar a súa identidade. Accede con frecuencia a servizos en liña que exixen autenticación e actualmente emprega varios métodos para verificar a súa identidade ao acceder a estes servizos. Ao usuario tamén lle preocupa compartir datos de identificación persoal (PID) durante as interaccións en liña. Os seus obxectivos inclúen identificarse con servizos que requiren a identificación do usuario e manter o control sobre o intercambio de datos persoais.

Este caso de uso abrangue todo o ciclo de vida da Carteira IDUE desde o punto de vista do usuario, desde a obtención dunha Carteira válida ata a identificación e autenticación do usuario dentro dun servizo en liña. A descrición actual centrarase nun fluxo remoto viable do mesmo dispositivo (véxase a sección 6.4), no que un Usuario persoa física emprega un único dispositivo móbil tanto para securizar a sesión como para acceder á información do servizo.

3.2 Permiso de condución móbil

Un caso de uso significativo para a Carteira IDUE consiste en permitir aos usuarios adquirir, almacenar e mostrar un documento dixital como o carné de conducir móbil (movile Driving License, mDL) para demostrar a súa habilitación para conducir. Neste caso, o usuario utiliza a Carteira IDUE para presentar o permiso a un terceiro, como un axente de policía.

A descrición do caso de uso centrarase nos fluxos de proximidade supervisados e non supervisados, que implican escenarios en que o usuario se encontra físicamente cerca dunha parte informada, e o intercambio e divulgación de atributos mDL prodúcese utilizando tecnoloxías de proximidade (por exemplo, NFC, Bluetooth). Os dous fluxos de proximidade teñen unha diferenza significativa: no fluxo *supervisado*, a Carteira IDUE presenta os atributos mDL a unha parte Informada humana ou baixo a súa supervisión (con axuda dun dispositivo); mentres que, no fluxo *non supervisado*, a Carteira IDUE presenta os atributos mDL a unha máquina sen supervisión humana.

3.3. Outros casos de uso

En versións posteriores deste documento, os seguintes casos de uso detallaranse como modelos de servizo:

- *Saúde*

O fácil acceso aos datos sanitarios é crucial tanto en contextos nacionais como transfronteirizos. A Carteira IDUE pode permitir o acceso á ficha do paciente, receitas electrónicas, etc.

- *Formación e cualificacións profesionais*

Facilitar documentos para os procedementos de validación de cualificacións pode resultar custoso e levar moito tempo aos usuarios finais, empresas e empregadores, provedores de educación e formación e outras institucións académicas. Por exemplo, os testemuños dixitais de diplomas poderíanse presentar de forma transfronteiriza nun formato verificable, fiable e consumible a outra institución educativa ou de formación ou a un posible empregador. A carteira IDUE permite recoller credenciais dixitais educativas en forma de testemuños electrónicos de atributos facilitando que os alumnos as recompilen e as presenten.

- *Finanzas dixitais*

A carteira IDUE facilitará o cumprimento dos requisitos de autenticación reforzada do cliente en contornos financeiros. En consonancia coa Estratexia de Pagamentos Retallistas da Comisión[10]o caso de uso desenvolverase en estreita coordinación cos grupos consultivos dos Estados membros sobre pagamentos retallistas e co sector financeiro.

[10] Comunicación da Comisión ao Parlamento Europeo, ao Consello, ao Comité Económico e Social Europeo e ao Comité das Rexións sobre unha estratexia de pagamentos retallistas para a UE COM/2020/592 final.

- *Credencial dixital de viaxe*

A Carteira IDUE pode almacenar credenciais dixitais de viaxe que lles permiten aos usuarios beneficiarse de viaxes máis fluídos.

Este traballo poderase ampliar no futuro a outros casos de uso.

4. Ecosistema europeo de carteiras de identidade dixital

Este capítulo describe o ecosistema da Carteira IDUE tal e como está previsto na proposta lexislativa da Comisión Europea para a reforma do Regulamento UE 910/2014.

4.1. Funcións no ecosistema

As funcións do ecosistema Carteira IDUE descríbense na Figura 1 e detállanse nas seccións seguintes.

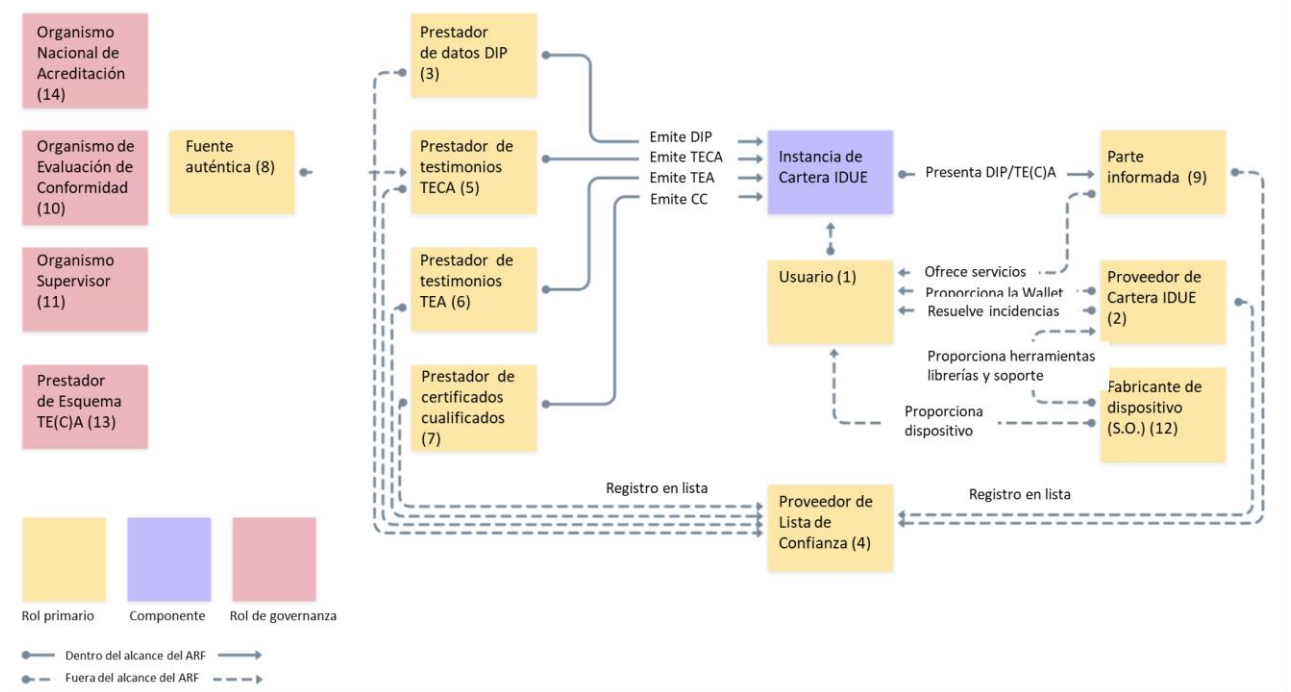


Figura 1: Visión xeral das funcións da carteira IDUE

1. *Usuarios finais das Carteiras IDUE*
2. *Proveedores de Carteras IDUE*
3. *Provedores de Datos de Identificación de Persoas*
4. *Provedores de Listas de Confianza*
5. *Provedores de testemuños electrónicos cualificados de atributos (TECA/QEAA)*
6. *Provedores testemuños electrónicos no cualificados de atributos (TEA/EAA)*
7. *Provedores cualificado ou non cualificados de certificados de sinatura electrónica/selo electrónico*
8. *Fuentes auténticas*
9. *Partes informadas*
10. *Organismos de Avaliación da Conformidade (OEC)*
11. *Organismos de supervisión*
12. *Fabricantes de dispositivos e provedores de subsistemas relacionados*
13. *Proveedores de esquemas de testemuños TEA/EAA o TECA/QEAA*
14. *Organismos nacionais de acreditación*

4.1.1. Usuarios de Carteira IDUE

Os usuarios de Carteiras IDUE utilizan a Carteira IDUE para recibir, almacenar e presentar testemuños (DIP/PID, TECA/QEAA ou TEA/EAA) sobre si mesmos, mesmo para demostrar a súa identidade. Os usuarios poden crear sinaturas e selos electrónicos cualificados (QES) utilizando unha Carteira IDUE.

En función da lexislación nacional determínase quen pode ser usuario dunha carteira IDUE. O uso dunha carteira IDUE non é obrigatorio para os cidadáns segundo a proposta de revisión do Regulamento eIDAS. Porén, os Estados membros están obrigados a ofrecer polo menos unha solución de carteira IDUE aos seus cidadáns.

4.1.2. Provedor de carteiras IDUE

Os provedores de carteiras IDUE son Estados membros ou organizacións autorizadas ou recoñecidas polos Estados membros que poñen a carteira IDUE á disposición dos usuarios derradeiras. Correspóndelle a cada Estado membro determinar os termos e condicións do mandato ou recoñecemento.

Os provedores de carteiras IDUE poñen á disposición dos usuarios a través dunha solución de carteira IDUE unha combinación de varios productos e servicios de confianza previstos na proposta de revisión do Regulamento eIDAS, que dan ao Usuario o control total sobre o uso dos seus Datos de Identificación de Persoa (DIP/PID) e Testemuños Electrónicos de Atributos Cualificados ou non Cualificados (TECA/QEAA ou TEA/EAA), e calquera outro dato persoal dentro da súa Carteira IDUE. Desde un punto de vista técnico, isto tamén pode implicar garantir ó Usuario o control exclusivo sobre o material criptográfico sensible (por exemplo, claves privadas) relacionado co uso destes datos nalgúns escenarios, incluída a identificación electrónica, ou a realización de sinaturas ou selos electrónicos.

Os provedores de carteiras IDUE son responsables de garantir o cumprimento dos requisitos para as carteiras IDUE.

4.1.3. Provedores de Datos de Identificación da Persoa (DIP/PID)

Os provedores de DIP/PID son entidades de confianza responsables de:

- verificar a identidade do Usuario de Carteira IDUE de conformidade cos requisitos de Nivel de Aseguramento Alto (LoA high),
- expedir DIP/PID á Carteira IDUE nun formato común harmonizado e
- facilitar información[11] para que as partes informadas verifiquen a validez do DIP/PID.

Correspóndelle a cada Estado membro determinar as condicións destes servizos.

Os provedores de DIP/PID poden ser, por exemplo, as mesmas organizacións que hoxe en día expiden documentos de identidade oficiais, medios de identidade electrónicos, provedores de carteiras IDUE, etc. Os provedores de carteiras IDUE poden ser ou non as mesmas organizacións que os provedores de DIP/PID.

[11] Sen prexuízo do mecanismo concreto polo que se facilite a información, xa sexa directa ou indirectamente

4.1.4. Provedores de listas de confianza

O estatus específico dun rol no ecosistema Carteira IDUE deberá poder ser verificado de forma fidedigna. Tales roles son:

- Proveedores de carteiras IDUE
- Provedores de Datos de Identificación de Persoas
- Provedores de testemuños electrónicos de atributos cualificados (TECA/QEAA)
- Provedores de Certificados cualificados para sinatura e selo electrónicos (CC/QC)
- Partes informadas (en certas ocasións, partes que Confían)
- Provedores non cualificados de testemuños electrónicos de atributos (TEA/EAA)
- Provedores de certificados non cualificados para sinatura e selo electrónicos
- Provedores doutros servicios de confianza
- Catálogos de atributos e esquemas para provedores de testemuño de atributos

Outras funcións poden ser necesarias e, por tanto, débense definir e mencionar explicitamente en función da función específica e da súa criticidade, por exemplo, as diferentes funcións e actores implicados nos procesos de sinatura a distancia.

Cando se utiliza, unha Lista de Confianza[12] debe contar cun mecanismo que permita incorporar ou retirar información sobre as entidades fiables do ámbito concreto a que se refire mantendo o rexistro de tales entidades e proporcionando a terceiros a súa información. Correspóndelle a cada entidade xestora dunha lista de confianza (rexistrador) establecer as condicións que deben cumprir as entidades para figurar na lista, polo menos que veñan predeterminadas por unha normativa xa existente, por exemplo, en normativa sectoriais.

4.1.5. Provedores de testemuño electrónico cualificado de atributos

Os testemuños TEA/EAA cualificados as prestan os PCSC (Prestadores Cualificados de Servizos de Confianza, en inglés QTSP, Qualified Trust Service Providers). O marco de confianza xeral para os PCSC aplícase tamén aos TECA/QEAA, pero tamén cómpre definir normas específicas para este servizo de confianza. Os provedores de TECA/QEAA manteñen unha interface para solicitar e proporcionar TECA/QEAA, incluída unha interface de autenticación mutua coas carteiras IDUE e, potencialmente, unha interface cara fontes auténticas para verificar atributos. Os provedores de TECA/QEAA proporcionan información ou a situación dos servizos que se poden utilizar para preguntar sobre o estado de validez dos TECA/QEAA, sen poder recibir ningunha información sobre o uso dos testemuños. Correspóndelle a cada PCSC determinar os termos e as condicións destes servizos, máis alá do especificado no Regulamento eIDAS.

4.1.6. Provedores de testemuño electrónico non cualificado de atributos

[12] Máis adiante achegaranse máis precisións sobre cómo se poderían aplicar as listas de confianza.

Os TEA non cualificados os poden proporcionar provedores de servizos de confianza cualificados ou non cualificados. Aínda que están supervisados segundo o marco regulatorio de eIDAS, cabe supoñer que outros marcos xurídicos ou contractuais distintos da eIDAS rexen na súa maioría as normas de prestación, uso e recoñecemento dos TEA xa existentes.

Estes outros marcos poden abranguer áreas de política como os permisos de conducir, credenciais educativas ou pagamentos dixitais, aínda que tamén poden recorrer a provedores cualificados de testemuño electrónico de atributos. Para que se utilicen os TEA, os PSC/TSP ofrecen aos usuarios unha forma de solicitar e obter TEA, o que significa que deben cumprir tecnicamente as especificacións da interface de Carteira IDUE. Dependendo das regras do dominio, os provedores de TEA/EAA poden proporcionar información sobre a validez dos TEA/EAA, sen ter a posibilidade de recibir ningunha información sobre o uso que a parte Informada fará dos TEA/EAA. As condicións de emisión dos TEA e os servizos conexos están suxeitos a normas sectoriais.

Os prestadores cualificados e non cualificados de DIP/PID, TEA/EAA e TECA/QEAA tamén poden recibir a denominación de **partes informantes**, por contraste coas *partes que confían* nos testemuños que reciben e se denominan tamén **partes informadas**.

4.1.7. Prestadores de certificados cualificados e non cualificados para sinaturas e selos electrónicos

O número 3 do artigo 6 bis do texto denominado "COM(2021)281 final" que contén a proposta de modificación do Regulamento eidas exixe que a carteira IDUE permita ao usuario crear sinaturas ou selos electrónicos cualificados. Este obxectivo pódese acadar de varias maneiras:

- La carteira IDUE está certificada como dispositivo cualificado de creación de firma o sello (DCCF o DCCS, en inglés Qualified Signature/Seal Creation Device, QSCD), o ben
- Implementa capacidades seguras de autenticación e invocación para a realización de sinatura/selo como parte dun DCCF/QSCD local ou un DCCF/QSCD remoto xestionado por un PCSC/QTSP.

As interfaces de Carteira IDUE cos DCCF/QSCD ampliaranse en futuras versións deste documento ARF.

4.1.8. Provedores doutros servicios de confianza

A interacción de carteira IDUE con provedores doutros servicios de confianza cualificados ou non cualificados, como os selos de tempo, poderase describir con máis detalle en futuras versións deste documento ARF.

4.1.9. Fontes auténticas

As fontes auténticas son os repositorios ou sistemas públicos ou privados recoñecidos ou esixidos pola lei que conteñen atributos sobre unha persoa física ou xurídica. As fontes auténticas no ámbito do anexo VI da proposta de revisión do Regulamento eIDAS son fontes de atributos sobre dirección, idade, sexo, estado civil, composición familiar, nacionalidade, títulos e licenzas de educación e formación, títulos e licenzas de cualificacións profesionais, permisos e licenzas públicos, datos financeiros e empresariais. As fontes auténticas incluídas no ámbito de aplicación do anexo VI deben proporcionar interfaces aos provedores de TECA/QEAA para verificar a autenticidade dos atributos mencionados, xa sexa directamente ou a través de intermediarios designados recoñecidos a nivel nacional. As fontes auténticas tamén poden emitir testemuños TE(C)A/(Q)EAA por si mesmas se cumpren os requisitos do Regulamento eIDAS. Correspóndelles aos Estados membros definiren os termos e condicións para a prestación destes servizos, pero de acordo coas especificacións técnicas, normas e procedementos mínimos aplicables aos procedementos de verificación dos testemuños electrónicos cualificadas de atributos.

4.1.10. Partes Informadas (o Partes que confían)

As partes informadas son persoas físicas ou xurídicas que confían nunha identificación electrónica ou nun servicio de confianza. No contexto das carteiras IDUE, solicitan os atributos necesarios contidos no conxunto de datos DIP/PID, TECA/QEAA e TEA/EAA dos usuarios de carteiras IDUE para confiar na carteira IDUE, logo de aceptación por parte do propietario da carteira (usuario) e dentro dos límites da lexislación e as normas aplicables. A razón para confiar na carteira IDUE pode ser un requisito legal, un acordo contractual ou a propia decisión da entidade informada. Para recibir información dunha Carteira IDUE, as partes informadas deben notificar ao Estado membro en que están establecidas sobre a súa intención de recibir información procedente de Carteiras IDUE. As partes que confían deben manter unha interface con Carteira IDUE para solicitar testemuños con autenticación mutua. As partes Informadas son responsables de autenticar os DEP/PID e os TE(C)A/(Q)EAA.

4.1.11. Organismos de avaliación da conformidade (OEC)

As carteiras IDUE deben estar certificadas por organismos públicos ou privados acreditados designados polos Estados membros[13]. Os PCSC deben ser auditados periodicamente por organismos de avaliación da conformidade (OEC, en inglés, CAB, Conformity Assessment Bodies). Os OEC/CAB están acreditados por un organismo nacional de acreditación de conformidade co Regulamento 765/2008 como responsables de levar a cabo as avaliacións en que os Estados membros terán que se exceder antes de expedir unha carteira IDUE ou proporcionar o estatus de "cualificado" a un provedor de Servizos de Confianza. As normas e

[13] Artigo 6 quater, número 3

réximes utilizados polos OEC/CAB para desempeñar as súas tarefas de avaliación/homologación das carteiras IDUE especifícanse máis adiante no proceso "Toolbox".

4.1.12. Organismos de supervisión

Os Estados membros deben notificarlle á Comisión Europea a designación de organismos de supervisión cuxa misión é supervisar aos PCSC/QTSP e actúan, en caso necesario, en relación cos provedores de servizos de confianza non cualificados.

4.1.13. Fabricantes de dispositivos e entidades relacionadas

As carteiras IDUE disporán de varias interfaces cos dispositivos en que se baseen, que poderán ter as seguintes finalidades:

- Almacenamento local.
- Acceso a Internet en liña.
- 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.
- Tarxetas intelixentes e elementos seguros (SE, compoñente de smartphone).

Para o almacenamento seguro de material criptográfico, pódese establecer unha interface con dispositivos ou servizos específicos. Outras entidades relacionadas poden ser provedores de servizos, como provedores de servizos na nube, provedores de tendas de aplicacións App, etc.

A proposta legal de reforma do regulamento EIDAS establece restricións (por exemplo, o cumprimento de Nivel de Aseguramento Alto – "LoA high") respecto a qué tipos de dispositivos e servizos pódense utilizar co fin de emitir o Carteira IDUE. Do mesmo modo, a dispoñibilidade, así como os termos e condicións dos provedores de interfaces de dispositivos e provedores de servizos relacionados, establecerán outras restricións para os provedores de carteiras IDUE.

4.1.14. Provedores de esquemas de testemuños electrónicos de atributos cualificado e non cualificados

Os provedores de esquemas TE(C)A/(Q)EAA publican esquemas e vocabularios que describen a estrutura e a semántica dos testemuños TE(C)A/(Q)EAA. O que pode permitir a outras entidades, como as partes informadas, o descubrimento e validación dos TE(C)A/(Q)EAA. A Comisión Europea establece as especificacións técnicas, normas e procedementos mínimos para tal efecto. A existencia de esquemas comúns, mesmo por parte de organizacións sectoriais específicas, é fundamental para a adopción xeneralizada dos TE(C)A/(Q)EAA.

4.1.15. Organismos nacionais de acreditación

Os organismos nacionais de acreditación (ONA, en inglés NAB, National Accreditation Bodies) de acordo co Regulamento (CE) nº 765/2008[14] son os organismos dos Estados membros que realizan a acreditación con autoridade derivada do Estado membro. Os ONA/NAB acreditan os OEC/CAB como organismos de certificación profesional competentes, independentes e supervisados encargados de certificar produtos/servizos/procesos facendo uso de documento(s) normativo(s) que establecen os requisitos (por exemplo, lexislacións, especificacións, perfís de protección, normas técnicas). Os ONA/NAB supervisan os OEC/CAB aos que expediron un certificado de acreditación.

4.2. Ciclo de vida dunha carteira IDUE

O texto de proposta de reforma do Regulamento eIDAS define a carteira IDUE cun alto nivel de abstracción, así como aos provedores de carteiras IDUE que teñen a obriga legal de garantir que os habitantes/residentes dun Estado membro poidan obter unha carteira IDUE valido e plenamente funcional. O ciclo de vida dunha Carteira IDUE terá algunhas interaccións cos provedores de Listas de Confianza que especifican o estado dun rol no ecosistema de Carteiras IDUE dunha maneira fiable. Desenvolver unha Arquitectura e un marco de Referencia que deben servir de guía para o desenvolvemento da dita carteira IDUE require un nivel de abstracción máis detallado para ser eficiente e producir unha descrición da arquitectura o suficientemente expresiva como para ser prescritiva.

Este capítulo parte dun modelo de obxectos mínimo e define o ciclo de vida dos conceptos centrais: Solución de Carteira IDUE, DEP/PID, TE(C)A/(Q)EAA e Instancia de Carteira IDUE. Eses conceptos elixíronse como punto de partida porque o desenvolvemento conxunto do ARF mostrou que os ciclos de vida destes conceptos están estreitamente entrelazados, o que levou a unha descrición pouco clara e, en consecuencia, provocou malentendidos.

O modelo de obxectos ampliarase segundo sexa necesario en futuras versións do ARF.

4.2.1. Modelo simplificado de carteira IDUE

Na Figura 2 distínguense os conceptos de Solución de Carteira IDUE e Instancia de Carteira IDUE. Unha Solución Carteira IDUE é o produto e/ou servizo completo proporcionado por un Provedor de Carteira IDUE. Unha Instancia de Carteira IDUE é unha instancia persoal dunha solución Carteira IDUE que se executa nun dispositivo do usuario ao que pertence e que é quen a controla.

[14] Regulamento (CE) nº 765/2008 do Parlamento Europeo e do Consello, do 9 de xullo de 2008, polo que se establecen os requisitos de acreditación e vixilancia do mercado relativos á comercialización dos produtos e polo que se derroga o Regulamento (CEE) nº 339/93.

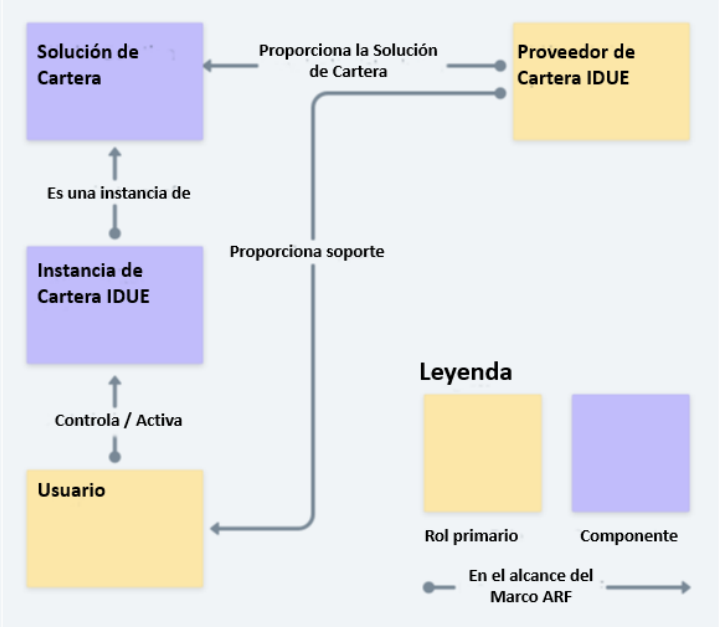


Figura 2: Modelo simplificado de obxectos de carteira IDUE

Esta definición non é prescritiva do factor de forma, polo que, dependendo da implementación, unha Instancia de Carteira IDUE pode consistir nunha única aplicación móbil, ou nun conxunto de compoñentes locais e remotos dispoñibles para un usuario específico.

4.2.2. Ciclos de vida dos DEP/PID e dos TE(C)A/(Q)EAA

Os ciclos de vida dos DIP/PID e dos TE(C)A/(Q)EAA son esencialmente idénticos, sen embargo, para o alcance desta descrición nos referiremos posteriormente só á EPI. O texto desta sección aplicado á EPI aplícase mutatis mutandis aos TE(C)A/(Q)EAA.

O DEP/PID no contexto da Carteira IDUE comeza o seu ciclo de vida cando se emite a unha Instancia de Carteira IDUE. Teña en conta que isto significa que a xestión de atributos na fonte auténtica (respectando as estruturas nacionais e as definicións de atributos) queda fóra do ámbito do ARF.

Hai que ter en conta que, para determinados casos de uso, os DIP/PID poden estar aprovisionados, o que significa que aínda non son válidos cando se emiten, pero acadan a súa validez máis tarde. Se os DIP/PID se emiten na data de inicio de validez ou despois, considérase inmediatamente que o estado cambia directamente a válido se a data de comprobación é posterior á de inicio de validez. Isto significa que os DIP/PID poderían estar "preemitidos".

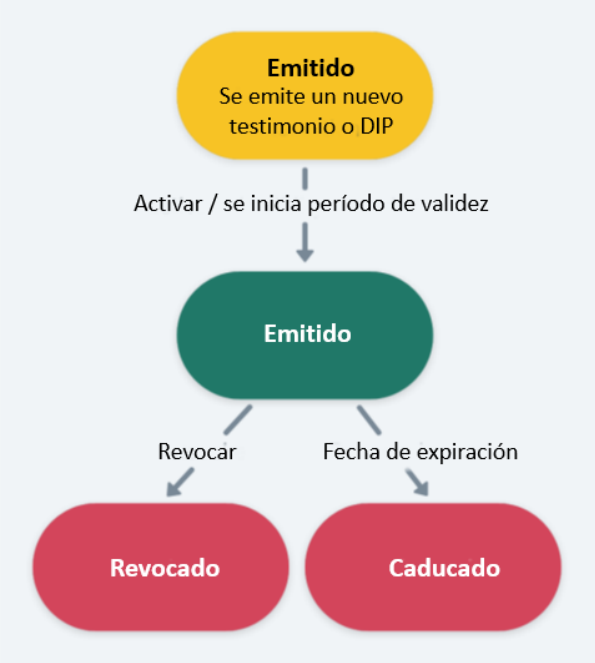


Figura 3: Diagrama de estados do DIP/PID

Existen dúas transicións posibles dun DIP/PID válido: ou ben expira automaticamente, por superarse a *"data de fin de validez*", ou ben é revogado activamente polo seu Provedor antes da súa expiración. A expiración e a revogación son transicións esencialmente independentes. Unha vez que o DIP/PID caducou ou se revogou, non pode volver ser válido. A actualización do DIP/PID (por exemplo, debido a un cambio de nome) sempre require unha nova emisión.

4.2.3. Ciclo de vida da solución carteira IDUE

Unha Solución Carteira IDUE ten un estado propio, tal e como se define no artigo 10 bis do futuro regulamento. O estado da Solución afecta ao estado de todas as instancias de carteira IDUE da dita Solución de Carteira IDUE. O estado "**Candidato"** é o primeiro estado dunha Solución Carteira IDUE. Isto significa que está totalmente implementada e que o Provedor de Carteiras IDUE solicita que a solución se certifique como Carteira IDUE.

Se se cumpriron todos os criterios legais e técnicos, incluída a certificación da Solución Carteira/Wallet polo OEC/CAB, entón un Estado membro pode decidir empezar a proporcionar **Instancias** da Solución aos Usuarios. O estado da Solución pasa a ser "**válido"**. De conformidade co artigo 6 quinquies, o Estado membro informará a Comisión de calquera cambio no estado de certificación da súa Solución Carteira/Wallet. Isto significa que a solución carteira IDUE pódese lanzar **oficialmente** e que se poden proporcionar instancias da solución aos usuarios.

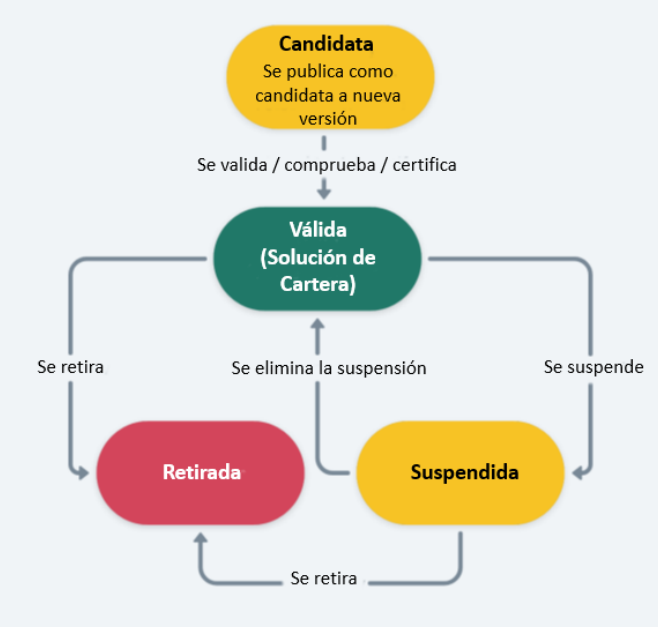


Figura 4: Diagrama de estado da solución Carteira/Wallet

Nas condicións legais do artigo 10 bis, número 1, o Estado membro emisor pode suspender temporalmente unha Solución Carteira IDUE. Isto podería ser, por exemplo, como consecuencia dun problema crítico de seguridade nesa solución Carteira IDUE. Isto dá lugar ao estado de "**suspendida**". De conformidade co número 2 do artigo 10 bis, o Estado membro emisor pode cancelar a suspensión da Solución Carteira/Wallet e continuar coa emisión, devolvendo a Solución ao estado "**válido**". De conformidade co número 3, a solución Carteira IDUE pódese retirar e cancelar por completo.

4.2.4. Ciclo de vida da instancia de carteira IDUE

Unha Instancia de Carteira IDUE comeza a súa vida superá nunha Solución de Carteira IDUE válida. O provedor de Carteira IDUE proporciona unha Solución de Carteira IDUE ao Usuario que se considera que executa unha Instancia de Carteira en estado "**operativo**" unha vez instalada e activada polo Usuario no seu dispositivo. Dependendo do factor de forma e da implementación, proporcionar unha instancia pode requirir varias accións, por exemplo, instalación e inicialización no caso dunha Carteira IDUE móbil. Unha Instancia de Carteira IDUE deste tipo podería utilizarse xa para funcións non específicas de IDUE, como almacenar tarxetas de fidelidade ou billetes de tren non personalizados ou calquera outro certificado que non esixa a vinculación a uns DIP/PID válidos.

Unha vez que se inicializa unha Instancia de Carteira IDUE, considérase "**válida**", o que significa que é recoñecida por un Provedor de DIP/PID e que posúe un conxunto de DIP/PID válidos. Se os DIP/PID caducan ou se revogan, a Carteira IDUE non queda automaticamente inutilizada, senón que o seu estado rebaixado a "**operativo**". Isto pode afectar a validez dun testemuño TE(C)A/(Q)EAA ou dun certificado cualificado para asina ou selos electrónicos.

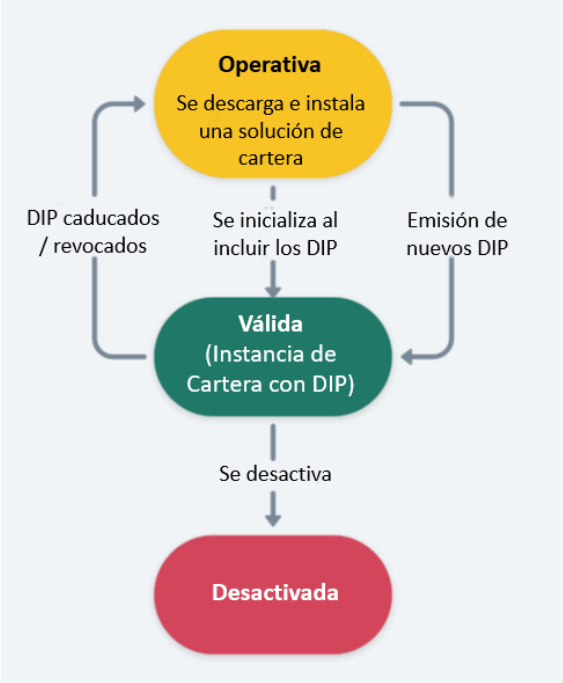


Figura 5: Diagrama de estado da instancia de carteira

Actualmente asúmese que só o Usuario[15] poderá desactivar unha Instancia de Carteira IDUE. Hai que ter en conta que isto é independente da posibilidade de que un prestador de datos DIP/PID ou un provedor de testemuño TE(C)A/(Q)EAA revoguen os seus testemuños.

[15] Por exemplo, en caso de falecemento do usuario ou de vulnerabilidade da seguridade de Carteira IDUE.

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

5.1. Datos de identificación da persoa

Neste capítulo detállase o conxunto DEP/PID presentado pola Carteira IDUE.

Un provedor de DIP/PID pode emitir un conxunto de datos DIP/PID para a carteira IDUE e permitir o uso da carteira IDUE como medio de identificación electrónica ao acceder a servizos en liña e fóra de liña.

Os mecanismos a través dos cales se xera o DIP/PID e proporciónase á Carteira IDUE dependen dos Estados membros e só están limitados por requisitos legais como os requisitos de nivel de aseguramento (LoA High), RGPD/GDPR ou calquera outra lei nacional ou da Unión Europea.

A continuación describirase o formato dos datos tal e como se presentan á parte usuaria, sen facer ningunha suposición sobre cómo a carteira IDUE recuperou ou xerou estes datos de antemano.

5.1.1 O conxunto de datos

5.1.2.1. Principios para a revisión do conxunto DIP/PID

Este capítulo propón unha revisión dos conxuntos de datos opcionais eIDAS especificados na norma derivada de eidas "CIR 2015/1501"[16] e analízanse outras especificacións, a minimización de datos e os identificadores.

A revisión do conxunto de datos opcionais eIDAS que aquí se propón se constrúe sobre a base dos seguintes principios:

- Non debe haber dúas persoas co mesmo conxunto de atributos obrigatorios DIP/PID.
- O conxunto de DIP/PID debe conter polo menos o conxunto mínimo de atributos especificados no Regulamento de execución "CIR 2015/1501" como obrigatorios.

[16] Regulamento de Execución (UE) 2015/1501 da Comisión, do 8 de setembro de 2015, relativo ao marco de interoperabilidade de conformidade co artigo 12, número 8, do Regulamento (UE) n.º 910/2014 do Parlamento Europeo e do Consello, relativo á identificación electrónica e os servizos de confianza para as transaccións electrónicas no mercado interior.

- O conxunto de datos obrigatorios limítase por natureza á intersección (estreita) do que todos os Estados membros poden proporcionar para todas as persoas físicas e xurídicas e o que se necesita para efectos de identificación electrónica.

5.1.1.1. Atributos do DIP/PID para persoas físicas

A seguinte táboa ofrece unha visión xeral dos atributos DEP/PID incluídos actualmente no marco eIDAS, así como dos atributos opcionais adicionais que se suxire incluír.

Atributos eIDAS obrigatorios	Atributos eIDAS opcionais	Posibles atributos opcionais adicionais
Apellido(s) actual	**Apelido(s) de nacemento**	**Nacionalidade/Cidadanía***
Nomes actuais	**Nomes de nacemento**	
Data de nacemento	**Lugar de nacemento**	**Atributos opcionais utilizados a nivel nacional, por exemplo, número de identificación fiscal, número da seguridade social, etc.**
Identificador único	**Dirección actual**	
	Género	

Cadro 2 - Atributos obrigatorios e opcionais do diP/PID para as persoas físicas

**Nacionalidade/Cidadanía - trátase dun posible atributo multiplicador porque os cidadáns poden ter máis dunha nacionalidade. Porén, a nacionalidade/cidadanía tamén se pode comunicar en forma de TE(C)A/(Q)EAA, para permitir aos cidadáns demostrar unha nacionalidade determinada, sen actualizar o conxunto de DIP/PID nin implicar ao provedor de DIP/PID.*

Engadíronse posibles atributos opcionais adicionais para facilitar unha gama máis ampla de opcións de autenticación tanto en liña como fóra de liña, así como para abordar a aprendizaxe derivada das actuais implementacións de eIDAS.

Os metadatos asociados aos DEP/PID poden detallar adicionalmente a data de emisión e/ou caducidade, a autoridade emisora e/ou o Estado membro, a información necesaria para realizar a vinculación do titular e/ou a proba de posesión, a información ou localización dos servizos que se poden utilizar para consultar o estado de validez dos atributos e potencialmente máis información.

5.1.2 Requisitos de expedición do EPI

No cadro seguinte defínense os requisitos aplicables aos DEP/PID en relación coa información que se inclúe no certificado, por exemplo, para efectos de comprobación de validez, autenticidade, validación, políticas, modelo de datos e formatos.

As futuras versións deste texto poderán ampliar a táboa para especificar requisitos. Hai que ter en conta que estes requisitos están dirixidos principalmente á primeira versión das especificacións da solución Carteira IDUE, e que poden cambiar a medida que evolucionen as especificacións.

#	Requisito
1	**O testemuño sobre DEP/PID DEBE conter a información necesaria para identificar o provedor de DIP/PID.**
2	**O testemuño sobre DEP/PID DEBE conter a información necesaria para realizar unha comprobación da integridade dos datos.**
3	**O testemuño sobre DEP/PID DEBE conter a información necesaria para verificar a súa autenticidade.**
4	**O testemuño sobre DEP/PID DEBE conter toda a información necesaria para realizar comprobacións do estado de validez do testemuño.**
5	**O testemuño sobre DEP/PID DEBE incluír toda a información (como atributo ou como calquera outro valor asinado) necesaria para realizar a verificación da vinculación do titular por unha parte informada.**
6	**O testemuño sobre DEP/PID DEBE emitirse para ser presentada de acordo tanto co modelo de datos especificado na norma ISO/IEC 18013-5:2021 como co Modelo de datos de credenciais verificables v1.1 do W3C.**
7	**O testemuño sobre DEP/PID DEBE codificarse como CBOR e en formato JSON.**
8	**O testemuño sobre DIP/PID DEBE permitir a divulgación selectiva de atributos mediante o uso do esquema "Selective Disclosure for JWTs (SD-JWT)" e "Mobile Security Object (ISO/IEC 18013-5)" de acordo co modelo de datos (Permiso de conducir no móbil).**
9	**O testemuño sobre DIP/PID DEBE utilizar sinaturas electrónicas e formatos de cifrado tal e como se detalla na 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	**O testemuño sobre DIP/PID DEBE utilizar algoritmos de asinamento e cifrado de conformidade coa norma SOG-IS ACM (Agreed Cryptographic Mechanism)[17].**

Cadro 3 - Requisitos de expedición de EPI

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

5.2. Testemuño electrónico de atributo cualificado e non cualificado

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

No cadro seguinte defínense os requisitos aplicables aos Testemuños TE(C)A/(Q)EAA en relación coa información que se inclúe no Testemuño, por exemplo, para efectos de comprobación de validez, autenticidade, validación, políticas relacionadas coa xestión de claves, o modelo de datos e os formatos.

Os testemuños TE(C)A/(Q)EAA tamén se poden emitir de acordo cos requisitos aplicables aos Datos DIP/PID.

As futuras versións deste texto poderán ampliar a táboa para especificar requisitos. Hai que ter en conta que estes requisitos están dirixidos principalmente á primeira versión das especificacións da solución Carteira IDUE, e que poden cambiar a medida que evolucionen as especificacións.

#	Requisito
1	**Os testemuños TE(C)A/(Q)EAA DEBEN conter a información necesaria para identificar o Emisor.**
2	**Os testemuños TE(C)A/(Q)EAA DEBE Ncontener a información necesaria para realizar unha comprobación da integridade dos datos.**
3	**Os testemuños TE(C)A/(Q)EAA DEBEN conter a información necesaria para verificar a súa autenticidade.**
4	**Os testemuños TE(C)A/(Q)EAA DEBEN conter toda a información necesaria para realizar comprobacións do seu estado de validez.**
5	**(non se indica)**
6	**Os testemuños TE(C)A/(Q)EAA DEBERÍAN incluír toda a información (como atributo ou como calquera outro valor asinado) necesaria para realizar a verificación da vinculación do titular por parte dunha parte informada.**
7	**Os testemuños TE(C)A/(Q)EAA DEBEN expedirse de conformidade cunha das especificacións do modelo de datos: a norma de codificación de permiso de conducir: I"SO/IEC 18013-5:2021", o "Verifiable Credentials Data Model v1.1" (Modelo de datos de credenciais verificables 1.1) do W3C.**
8	**Os testemuños TE(C)A/(Q)EAA DEBERÍAN codificarse como un dos seguintes formatos: CBOR ou JSON segundo o modelo de datos utilizado para a certificación. Ver RFC 8812, RFC 8152, RFC 9052, RFC 9053**

9	**Os testemuños TE(C)A/(Q)EAA PODEN codificarse como JSON-LD (JSON for Linking Data).**
10	**Os testemuños TE(C)A/(Q)EAA DEBERÍAN permitir a Revelación Selectiva de atributos utilizando ben "Selective Disclosure for JWTs" (Revelación Selectiva para JWTs) (SD-JWT) ou ben o esquema "Mobile Security Object" (Obxecto de Seguridade Móbil) da norma sobre permiso de conducir (ISO/IEC 18013-5) de acordo co modelo de datos utilizado para o testemuño.**
11	**Os testemuños TE(C)A/(Q)EAA DEBERÍAN utilizar un dos seguintes formatos de sinatura e cifrado segundo se detalla nas normas do IETF, RFC relativas a JOSE (Javascript Object Signing and Encryptio), e RFCs relativas a COSE (CBOR Object Signing and Encryption) RFCs de acordo co modelo de datos utilizado para o testemuño.**
12	**Os testemuños TE(C)A/(Q)EAA DEBERÍAN utilizar algoritmos de cifrado de conformidade coa norma SOG-IS ACM (Agreed Cryptographic Mechanism)**
13	**Os testemuños TE(C)A/(Q)EAA DEBERÍAN emitirse de acordo co protocolo OpenID4VCI (OpenID for Verifiable Credential Issuance).**

Cadro 4 - Requisitos de expedición das (Q)CEA

6. Arquitectura de referencia e fluxos

A arquitectura de referencia representa un conxunto de decisións tomadas durante o proceso de deseño da arquitectura das solucións de Carteira IDUE. Estas eleccións basáronse na necesidade de que as solucións de Carteira IDUE soporten varios escenarios nos que o usuario, a parte que confía (ou parte informada), ou ambos, estean fóra de liña, ao tempo que proporcionan flexibilidade aos Estados membros para implementar unha solución de Carteira IDUE en varias configuracións de compoñentes.

6.1. Consideracións sobre o deseño

Para limitar a complexidade, as especificacións iniciais da Solución de Carteira IDUE incluirán só un número mínimo de compoñentes da solución que permitan o uso da Instancia de Carteira IDUE para a identificación do Usuario, de forma que poida funcionar como un medio de Identidade Electrónica (eID).

As opcións elixidas non reflicten unha importancia relativa nin un compromiso a longo prazo. No seu lugar, a selección guiouse por factores como a dispoñibilidade e madurez das normas e especificacións, unha estimación da facilidade de adopción e o grao de flexibilidade (en termos de casos de uso permitidos) que ofrece cada compoñente da solución.

Os compoñentes da solución aquí propostos evidencian a expectativa actual de utilizar a 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. Compoñentes de arquitectura

Os seguintes compoñentes foron identificados como os bloques de construción da arquitectura da carteira IDUE necesarios para implementar unha Solución de Carteira IDUE:

- **Sistema de xestión de claves criptográficas.** Este compoñente encárgase de xestionar e almacenar información criptográfica como as claves privadas xeradas, por exemplo, durante o proceso de emisión de DIP/PID.

- **Protocolo de intercambio de testemuños**. Este protocolo define cómo solicitar e presentar os datos DEP/PID e os testemuños TE(C)A/(Q)EAA de forma segura e preservando a privacidade. O protocolo tamén define cómo se realiza a autenticación entre a parte que Confía (ou Parte Informada) e a Instancia de Carteira IDUE, en particular o mecanismo a través do cal a parte Informada pode solicitar a identificación a través da Carteira IDUE. A solicitude contén toda a información necesaria sobre a parte informada e os datos solicitados. Este protocolo ocúpase da negociación da confianza e a autenticación mutua.

- **Protocolo de emisión**. O protocolo define cómo deben expedirse os DEP/PID e os testemuños TE(C)A/(Q)EAA e en qué formatos.

- **Modelo de datos**. O modelo de datos define e describe os elementos de datos e cómo interactúan entre si e as súas propiedades.

- **Esquemas DIP/PID e TE(C)A/(Q)EAA**. O esquema de testemuño contén a estrutura e a organización lóxica dos datos que definen as propiedades do testemuño, os atributos do Usuario. O esquema de testemuño tamén contén información adicional que inclúe, entre outras cousas, os mecanismos de verificación, a garantía de identidade subxacente (nivel de aseguramento) e o marco de confianza co que se relacionan as propiedades, así como a proba de posesión por parte do usuario lexítimo.

- **Formatos de DIP/PID e TE(C)A/(Q)EAA**. Os formatos de DIP/PID e TE(C)A/(Q)EAA utilízanse para representar a característica, cualidade, dereito ou permiso dunha persoa física ou xurídica ou dun obxecto, en forma de artefactos dixitais asinados electronicamente e verificables, que conteñen calquera propiedade adicional para efectos de interoperabilidade.

- **Formatos de asinamento**. Implementación técnica dun ou varios métodos matemáticos en forma de artefacto dixital, destinada a demostrar a autenticidade dun documento dixital, a súa integridade, autenticar o autor dun documento e, opcionalmente, tamén o seu destinatario (audiencia do documento).

- **Modelo de confianza.** Conxunto de normas que garanten a lexitimidade dos compoñentes e as entidades que interveñen na infraestructura de Carteira IDUE, e que abranguen:
  - Autenticación de usuarios.
  - Identificación do emisor.
  - Rexistro de emisores.
  - Modelos de datos e esquemas recoñecidos.
  - Rexistro e autenticación das partes informadas.
  - Mecanismos para establecer a confianza nun escenario multidominio.

  Os compoñentes do modelo de confianza permiten identifica-las entidades que confían en carteira IDUE e son fundamentais para a autenticidade, confidencialidade, integridade e o consentimento informado (nas sinaturas electrónicas e selos) da información. Existen diferentes modelos de confianza basados en distintas normas.

A lista de confianza é un mecanismo no marco dun modelo de confianza para publicar e obter información sobre partes que teñen autoridade, por exemplo, emisores de DIP/PID, de testemuños TE(C)A/(Q)EAA e partes informadas.

- **Suites e mecanismos criptográficos**. Algoritmos e métodos que aseguran o intercambio de datos en termos de confidencialidade e integridade.

- **Identificadores de entidade**. Identificadores únicos para todos os elementos do modelo de datos.

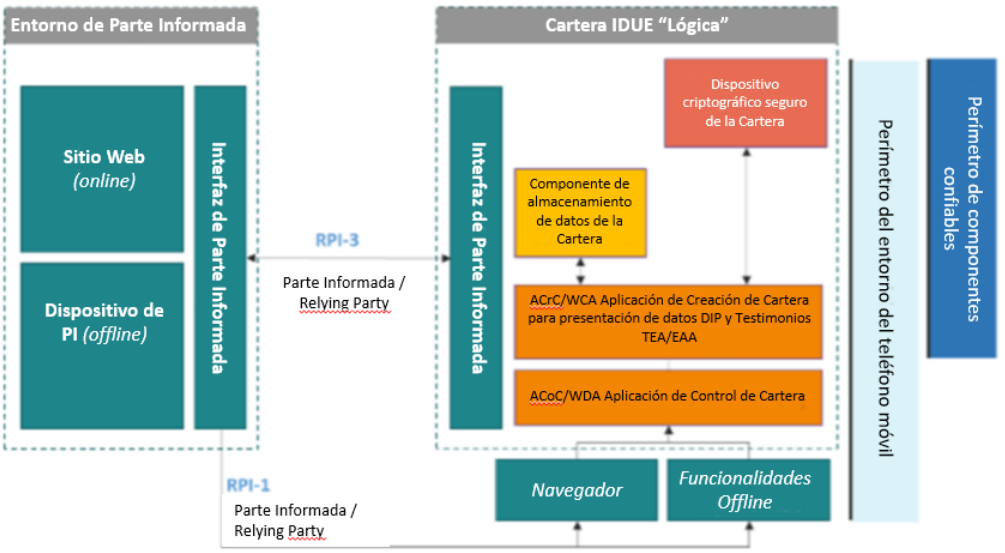
- **Comprobación do estado de validez**. Mecanismo para publicar e obter información sobre o estado de validez de, entre outros, de datos DIP/PID, de testemuños TE(C)A/(Q)EAA, certificados destinados a realizar sinaturas ou selos electrónicos, etc.

6.3. Arquitectura lóxica

Cando unha solución de Carteira IDUE ten unha aplicación que se executa nun dispositivo móbil, pode existir a necesidade de compoñentes de confianza adicionais que non forman parte desa aplicación pero que, sen embargo, forman parte dos recursos lóxicos da Carteira IDUE. Esta necesidade pode producir por varias razóns:

- Seguridade: por exemplo, se un dispositivo concreto non dispón de hardware suficientemente seguro, como un "Secure Element" (elemento seguro, equipamento estándar de moitos móbiles), poden ser necesarios compoñentes de hardware externos, como tarxetas intelixentes.
- Reutilización de sistemas en contornos de servidor remoto (backend).
- Reutilización da infraestrutura de identidade centrada no usuario (denominada a veces identidade descentralizada).

Estes compoñentes de confianza poden ser: almacenamento externo de confianza, hardware externo ou integrado de confianza ou outros compoñentes remotos de Carteira IDUEs. A continuación, amósase unha representación conceptual das variacións na implementación dos compoñentes de carteira IDUE:



ACRA/WCA: Crea a presentación (verificable) de DIP e Testemuños Cualificados que se comparten coa parte informada, segundo a información recibida da ACoC/WDA.
ACoC/WDA: Proporciona os datos elixidos polo usuario:

- DIP e testemuños (que se poden combinar)
- Determina cal se poden (ou non) presentar

Figura 6: Modelo conceptual das configuracións de Carteira IDUE

A táboa seguinte relaciona os compoñentes da carteira IDUE co modelo conceptual da figura 6.

Bloque funcional no modelo conceptual	Compoñentes aplicables á solución de Carteira IDUE
Dispositivo criptográfico seguro da Carteira IDUE	Claves de usuario e certificados
	Contorno seguro e illado para claves e datos
	Algoritmos criptográficos (por exemplo, simétricos, asimétricos, derivación de claves, funcións hash, xeración de números aleatorios) e protocolos (por exemplo, ECDH, TLS).
	Contorno seguro definido por hardwqre para claves e datos: un Elemento Seguro (SE), Contornos de Execución de Confianza (Trusted Execution Environment -TEEs), Módulo de Seguridade de Hardware (Hardware Security Module - HSM), etc. (remoto ou local).
	Datos de autenticación (PIN, biometría)
Compoñentes de almacenamento de datos da carteira IDUE	Identificador único e persistente do usuario
	Atributos do usuario
	Datos persoais e atributos do usuario
	Contorno seguro para claves e datos

Carteira IDUE "Presentación de DIP/PID o TEA/EAA" Aplicación de creación de Cartera (WCA - Wallet Creation Application)	Rexistros, historial de operacións da Instancia de Cartera IDUE, telemetría
	Identificador da Instancia de aplicación Carteira IDUE (por exemplo, configuración, fabricante e versión)
	Interfaces internas da instancia de Carteira IDUE (por exemplo, entre almacenamento, compoñentes, cifrado)
Aplicación de control de Cartera IDUE (WDA, Wallet Driving Application)	Rexistros, historial de operacións da Instancia de Cartera IDUE, telemetría
	Identificador da aplicación de Instancia de Carteira IDUE (por exemplo, configuración, fabricante e versión)
	Interfaz de usuario da Carteira IDUE
Interfaz da parte informada	Interface da Carteira IDUE con (Q)TSP, con provedores de TE(C)A/(Q)EAA, infraestruturas dos Estados membros, e-ID nacionais, partes que confían e outras fontes de EEA.
	Canles de comunicación (en liña/fóra de liña) entre a carteira IDUE e outras partes

Táboa 5 - Correspondencia entre os compoñentes da carteira IDUE e os bloques funcionais do modelo conceptual

A táboa seguinte asigna os compoñentes da Carteira IDUE aos dous perímetros representados na Figura 6.

Perímetros	**Compoñentes aplicables á solución Carteira IDUE**
Perímetros dos posibles compoñentes de confianza	Información sobre o dispositivo (tipo, configuración, versión de asinamento, estado, etc.)
	Claves e certificados do sistema
	Sistemas back-end (servidores de bases de datos)
	Dispositivos conectados de confianza
Perímetro móvil potencial	Información sobre o dispositivo (tipo, configuración, versión de asinamento, estado, etc.)
	Sensores del smartphone: cámara, lector NFC, sensor de huellas dactilares, acelerómetro, etc.

Cadro 6: correspondencia entre os compoñentes da carteira IDUE e os perímetros

6.4. Tipos de fluxos

Esta sección describe os catro tipos de fluxos que Carteira IDUE DEBE soportar a nivel xeral. Os catro fluxos son os seguintes:

1. Fluxo supervisado de proximidade.
2. Fluxo de proximidade non supervisado.
3. Fluxo remoto entre dispositivos.
4. Fluxo remoto do mesmo dispositivo.

Os fluxos 1 e 2 están relacionados cun escenario no que o usuario de Carteira IDUE se atopa físicamente cerca dunha parte que confía (parte informada) e o intercambio e a divulgación de testemuños (DIP/PID e/ou TECA/QEAA) deben producirse utilizando protocolos de proximidade (NFC, Bluetooth, QR-Code, etc.), sen que o usuario teña conectividade á internet (nótese que isto non implica que sexa posible calquera outra función áparte do transporte sen conexión). Os dous fluxos de proximidade difiren nun aspecto importante. No fluxo supervisado, a Carteira IDUE presenta atributos verificables a, ou baixo a supervisión de, unha persoa que actúa como parte informada (que pode operar un dispositivo propio). No fluxo non supervisado, a Carteira IDUE presenta atributos verificables a unha máquina sen supervisión humana.

Os fluxos 3 e 4 están relacionados cun escenario no que o intercambio de datos se debe producir a través da internet. Os dous fluxos remotos difiren nun aspecto importante. No fluxo remoto entre dispositivos, o usuario da Carteira IDUE consume información do servizo nun dispositivo distinto do dispositivo da Carteira IDUE, que só se utiliza para asegurar a sesión (por exemplo, utilizando Carteira IDUE para escanear un código QR nunha páxina de inicio de sesión para acceder a unha conta bancaria no seu navegador web). En cambio, no fluxo remoto do mesmo dispositivo, o usuario de Carteira IDUE utiliza o dispositivo da Carteira IDUE tanto para asegurar a sesión como para consumir a información do servizo.

As experiencias dos usuarios baséanse en polo menos un dos catro fluxos descritos, e probablemente nunha combinación de eles. Obsérvese que os catro fluxos se poden implementar de múltiples maneiras. As implementacións específicas quedan fóra do ámbito deste texto.

Cómpre seguir estudando os dous fluxos de proximidade, xa que son posibles con ou sen conexión á internet. Entre os posibles escenarios figuran:

- o Usuario e a parte Informada están ambos en liña,
- só o Usuario está conectado,
- só a parte Informada está en liña,
- O usuario e a parte informada están desconectados.

Para tódolos fluxos descritos anteriormente e, en concreto, para o fluxo non supervisado de proximidade, a autorización do usuario é un requisito previo para o intercambio de datos.

A continuación, detállanse as configuracións iniciais do DIP/PID e do TEA/EAA (no futuro poderanse engadir configuracións segundo sexa necesario).

6.5. Configuracións da carteira

6.5.1. Xustificación

Un dos obxectivos do desenvolvemento da Carteira IDUE é harmonizar os datos DIP/PID e os testemuños TE(C)A/(Q)EAA a través das fronteiras. Idealmente, isto implica un número moi reducido de solucións técnicas diferentes para limitar a complexidade, o que facilita a implantación e adopción. Por outra banda, a especificación de Carteira IDUE debe dar soporte a unha ampla gama de casos de uso con diferentes requisitos. Estas diferenzas motivan formas específicas de crear, solicitar e presentar datos DIP/PID e testemuños TE(C)A/(Q)EAA. Para satisfacer estas necesidades, as solucións de Carteira IDUE implementarán configuracións. Unha configuración é un conxunto específico de restricións e formas de utilizar as capacidades técnicas da Solución de Carteira IDUE para xestionar tanto o conxunto de DIP/PID como os testemuños TE(C)A/(Q)EAA.

O primeiro propósito dunha configuración é vincular as capacidades específicas da Carteira IDUE cos requisitos dos casos de uso que se poden cumprir con estas capacidades. Unha soa configuración debe soportar múltiples casos de uso; cada un conforme a configuración específica para a cal se emitiu o DIP/PID ou o testemuño TE(C)A/(Q)EAA.

O segundo e último propósito dunha configuración é proporcionar unha forramenta para ampliar potencialmente os contornos tecnolóxicos e as características das especificacións da Solución de Carteira IDUE. Se un caso de uso, ou un grupo de casos de uso, non se pode exceder nunha configuración existente da Solución de Carteira IDUE, introdúcese a necesidade de incluír unha configuración adicional para lles dar soporte aos requisitos que non se poden satisfacer coas configuracións existentes. No capítulo 8 descríbense a gobernanza e o proceso para engadir novas configuracións.

6.5.2. Configuracións iniciais

As solucións de Carteira IDUE admitirán inicialmente dúas configuracións:

- A configuración de **tipo 1** está dirixida especificamente aos casos de uso en que a parte Informada confía nas garantías requiridas para o nivel de aseguramento alto da identidade (LoA High), tal como se define no Regulamento de Execución CIR 2015/1502[18] para permitir a identificación transfronteiriza utilizando atributos DIP/PID en nivel de aseguramento da identidade (LoA High). A configuración de Tipo 1 está deseñada principalmente para fins de establecemento de datos de identidade DIP/PID.

[18] Regulamento de Execución (UE) 2015/1502 da Comisión, do 8 de setembro de 2015, polo que se establecen especificacións técnicas mínimas e procedementos relativos aos niveis de garantía dos medios de identificación electrónica de conformidade co artigo 8, número 3, do Regulamento (UE) n.º 910/2014 do Parlamento Europeo e do Consello, relativo á identificación electrónica e os servizos de confianza para as transaccións electrónicas no mercado interior.

- A configuración de **Tipo 2** ten como obxectivo permitir flexibilidade e soporte de características adicionais para posibles casos de uso de testemuños TE(C)A/(Q)EAA que non poidan ser satisfeitos pola configuración de Tipo 1 (por exemplo, posiblemente en áreas de saúde, credenciais de educación, ...).

Hai que ter en conta que a configuración de Tipo 1 non está pensada unicamente para o conxunto de DIP/PID. É probable que moitos testemuños TE(C)A/(Q)EAA se utilicen en ámbitos que requiran niveis de aseguramento altos (por exemplo, finanzas, sanidade, acceso a edificios) e teñan requisitos que se satisfagan coa configuración de Tipo 1. De ser así, estes TE(C)A/(Q)EAA expediranse de acordo coa configuración de Tipo 1.

6.5.3. Requisitos de configuración

Esta sección establece os requisitos das configuracións comparando a configuración de Tipo 1 e Tipo 2 en diferentes grupos de requisitos. As futuras versións deste texto poderán ampliar a táboa para especificar os requisitos relativos, por exemplo, aos emisores e ás partes que confían. Hai que ter en conta que estes requisitos están dirixidos principalmente á primeira versión das especificacións da Solución de Carteira IDUE, e que poden cambiar a medida que evolucionen as especificacións.

A seguinte táboa define os requisitos aplicables aos compoñentes da Solución de Carteira IDUE para soportar as dúas configuracións. Segundo o tipo de configuración o requisito implica substituír os puntos suspensivos [...] polo verbo indicado na columna Tipo 1 ou Tipo 2 (DEBE, DEBERÍA, etc).

Componente	**Requisito**	**Tipo 1**	**Tipo 2**
Sistema de xestión de claves criptográficas - 1	A Solución de Carteira IDUE [...] superarse nun dos seguintes compoñentes para almacenar e xestionar claves criptográficas: Elemento seguro (SE) integrado o contorno de (para dispositivos móbiles), dependencia dun dispositivo externo (elementos seguros / tarxetas intelixentes), e un servidor (módulo de seguridade de hardware remoto). A elección do hardware seguro que se utilizará e soportará depende de cada solución de Carteira IDUE.	DEBE	DEBERÍA

Sistema de xestión de claves criptográficas - 2	A Solución de Carteira IDUE [...] aplicar medidas de seguridade para evitar a exportación de segredos criptográficos.	DEBE	DEBERÍA
Protocolo de intercambio de testemuños - 1	La Solución de Cartera IDUE [...] soportar OpenID4VP como protocolo de intercambio de testemuños para **fluxos remotos.** Cando se solicita autenticación pseudónima, os parámetros de solicitude DEBERÍAN especificarse de acordo coa especificación OpenID SIOPv2.	DEBE	PODE
Protocolo de intercambio de testemuños - 2	A Solución de Carteira IDUE [...] soportar o protocolo detallado na norma ISO/IEC 18013-5:2021 para **fluxos de proximidade**.	DEBE	PODE
Protocolo de intercambio de testemuños - 3	A Solución de Carteira IDUE [...] realizar comprobacións para facer cumprir a vinculación de sesión (é dicir, solicitude de atributo para DIP/PID).	DEBERÍA	PODE
Protocolo de intercambio de testemuños - 4	La Solución de Cartera IDUE [...] soportar alternativas de protocolo de intercambio de testemuños[19].	PODE	PODE
Protocolo de intercambio de testemuños - 5	A Solución de Carteira IDUE [...] poder realizar unha proba de posesión.	DEBE	PODE
Protocolo de intercambio de testemuños - 6	A Solución de Carteira IDUE [...] soportar a Divulgación Selectiva de atributos tal e como se especifica na norma ISO/IEC 18013-5:2021.	DEBE	PODE
Protocolo de intercambio de testemuños - 7	A Solución de Carteira IDUE [...] soportar a Divulgación Selectiva de atributos como se especifica na especificación SD-JWT.	DEBE	PODE

[19] Cabe destacar a API REST de mdoc, tal e como se detalla no borrador e anorma ISO/IEC 23220-4.

Protocolo de emisión - 1**	La Solución de Cartera IDUE [...] admitir OpenID4VCI como protocolo de emisión. Os Estados membros son libres de incluír alternativas adicionais ao protocolo de emisión nas súas solucións nacionais.	DEBE **	DEBE
Modelo de datos -1	A Solución de Carteira IDUE [...] admitir testemuños emitidos de conformidade co modelo de datos especificado na norma ISO/IEC 18013-5:2021.	DEBE	DEBERÍA
Modelo de datos -2	A Solución de Carteira IDUE [...] soportar testemuños emitidos de acordo co modelo de datos especificado na especificación W3C Verifiable Credentials Data Model 1.1.	DEBE	DEBERÍA
Formatos DIP/PID y TE(C)A/(Q)EAA - 1	A Solución de Carteira IDUE [...] soportar testemuños en formato JWT e SD-JWT.	DEBE	PODE
Formatos DIP/PID y TE(C)A/(Q)EAA - 2	La Solución de Cartera IDUE [...] admitir testemuños en formato CBOR.	DEBE	PODE
Formatos DIP/PID y TE(C)A/(Q)EAA - 3	La Solución de Cartera IDUE [...] soportar testemuños en formato JSON-LD.	PODE	PODE
Formatos de firma -1	A Solución de Carteira IDUE [...] soportar formatos de asina electrónica e cifrado de acordo coas especificacións JOSE (JWT).	DEBE	PODE
Formatos de firma - 2	A Solución de Carteira IDUE [...] soportar formatos de asinamento e cifrado de acordo coas especificacións COSE.	DEBE	PODE
Formatos de firma - 3	A Solución de Carteira IDUE [...] admitir formatos de asinamento e cifrado de acordo coas especificacións LD-Proof.	NON DEBE	PODE

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

Táboa 7 - Requisitos de configuración

***Só para testemuños TE(C)A/(Q)EAA que deben ter un protocolo de emisión común para garantir a interoperabilidade. No caso dos datos DEP/PID, correspóndelle ao Estado membro definir o protocolo de emisión e cada solución de carteira soportará o protocolo de emisión de DEP/PID específico de acordo coas especificacións do Estado membro.*

As solucións de Carteira IDUE **DEBEN** soportar a configuración de **Tipo 1** que é obrigatoria para o DEP/PID.

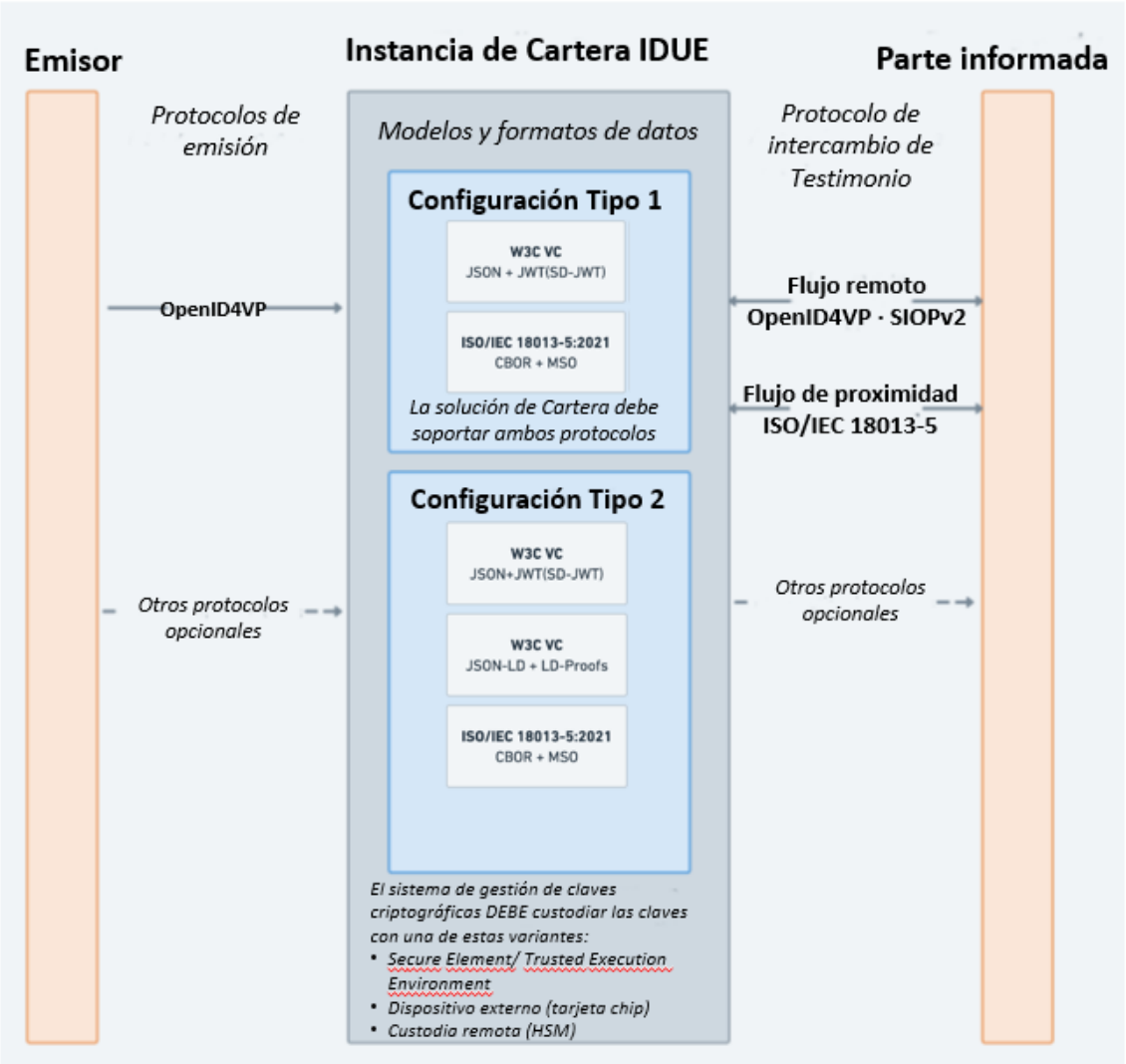


Figura 7. Configuracións Carteira IDUE.

7. O proceso de certificación das carteiras IDUE

Os Estados membros, de conformidade co artigo 6 quater (3) da proposta de reforma do Regulamento eIDAS, deben designar os organismos de avaliación da conformidade acreditados que supervisarán a realización da avaliación da conformidade das carteiras IDUE. Este proceso de designación débese harmonizar entre os Estados membros.

Unha vez efectuada esta designación, os Estados membros comunicaranlle á Comisión Europea os nomes e enderezos destes organismos públicos ou privados de acordo co número 5 do artigo 6 quater da dita proposta.
O provedor da carteira IDUE debe solicitar (seleccionar, contratar) a un ou varios OEC/CAB designados que avalíen e certifiquen a conformidade da súa carteira IDUE cos requisitos do Regulamento eIDAS.

A certificación da Carteira IDUE leva a cabo o OEC/CAB para avaliar e certificar a conformidade da Carteira IDUE (obxectivo da certificación) cos documentos normativos que deriven dos actos de execución establecidos no Art. 6a(11) sobre especificacións técnicas e operativas e normas de referencia.

A Carteira IDUE deberá estar certificada para garantir as avaliacións de conformidade, pero tamén para demostrar o cumprimento de altos niveis de seguridade. O uso dun sistema de certificación da ciberseguridade debería achegar un nivel harmonizado de confianza na seguridade da Carteira IDUE. Espérase que o almacenamento seguro de material criptográfico tamén estea suxeito á certificación de ciberseguridade.

O proceso de certificación dos provedores de carteiras IDUE debe aproveitar, baséarse e esixi-lo uso dos sistemas de certificación pertinentes e existentes do regulamento sobre a ciberseguridade, ou[20] partes destes, para certifica-la conformidade das carteiras, ou partes destes, cos requisitos de ciberseguridade aplicables.

[20] REGULAMENTO (UE) 2019/881 DO PARLAMENTO EUROPEO E DO CONSELLO do 17 de abril de 2019 relativo a ENISA (Axencia da Unión Europea para a Ciberseguridade) e á certificación da cidade.berseguridade das tecnoloxías da información e a comunicación e polo que se derroga o Regulamento (UE) n.º 526/2013 («Regulamento sobre a Ciberseguridade»)

8. Proceso de desenvolvemento da Arquitectura e do Marco de referencia

8.1. Publicación

Este documento e os elementos pendentes póñense á disposición do público na dirección electrónica https://code.europa.eu/eudi/architecture-and-reference-framework, onde se actualizará periodicamente segundo o fluxo de traballo descrito no capítulo 8.2.

8.2. Actualización

Para garantir un progreso constante e rápido na elaboración e actualización deste documento, aplícase o seguinte proceso e metodoloxía de traballo.

O Grupo de Expertos eIDAS (E03032)[21] deberá manter un backlog, que é unha lista priorizada de elementos de traballo para completar o ARF. A lista de tarefas pendentes actualizarase en función dos comentarios do Grupo de Expertos eIDAS, os proxectos piloto a Gran Escala impulsados desde a Axencia HaDEA (DIXITAL-2022-DEPLOY-02-ELECTRONIC-ID[22]), a Comisión ou outras partes interesadas, como as organizacións internacionais de normalización. Por exemplo, os resultados do desenvolvemento da implementación de referencia da Carteira IDUE (Framework Contract for Fixed Price and Quoted Time and Means for Development, Consultancy and Support for the European Dixital Identity Wallet[23]) e os conseguintes borradores de especificacións técnicas detalladas poden dar lugar a novos elementos de traballo.

A Comisión Europea (DG CONNECT) organizará o traballo sobre os temas atrasados e facilitará que o traballo avance segundo o calendario previsto.

O Grupo de Expertos de eIDAS debaterá e comparará periodicamente diferentes propostas relativas a solucións técnicas, recomendacións e requisitos relacionados con cada cuestión pendente pertinente con vistas a actualizar o ARF. A este respecto, o Grupo de Expertos eIDAS manterá unha lista de rexistros de decisións de arquitectura (RDA, en inglés ADR, Arquitecture Decission Records), de modo que sexa posible realizar un seguimento e comprender a motivación que subxace ás decisións técnicas descritas no ARF.

Calquera cambio e/ou actualización deste documento deberá ser acordado polo Grupo de Expertos eIDAS. O Grupo de Expertos eIDAS reunirase periodicamente co obxectivo 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

debater e aprobar novas versións deste documento, así como de actualizar os traballos pendentes de desenvolvemento.

Este documento adaptarase ao resultado das negociacións lexislativas da proposta de marco europeo de identidade dixital e actualizarase en consecuencia.

8.2.1. Versións de documentos

Para evitar problemas de interoperabilidade e que os cambios no ARF pasen desapercibidos, utilizarase para o ARF un sistema de control de versións e o seguinte esquema semántico de versións.

O documento ARF terá un número de versión determinado seguindo o formato *MAIOR. MENOR. PARCHE*, donde:

A versión **MAIOR** increméntase (é dicir, hai unha nova versión), cando o documento ARF sufriu cambios significativos, por exemplo, introducindo algúns cambios radicais na arquitectura,

A versión **MENOR** increméntase cando se engadiu nova información ao documento ou se eliminou información del, e

A versión **PARCHE** increméntase cando se realizaron cambios menores (por exemplo, corrección de erratas).

9. Referencias

[Palabras clave no ARF para indicar os niveis de esixencia] 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. e D. Chadwick, "Verifiable Credentials Data Model 1.0", 19 de novembro de 2019, <https://www.w3.org/TR/vc-data-model>.

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

[OpenID4VCI] Lodderstedt, T., Yasuda, K., e T. Looker, "OpenID for Verifiable Credential Issuance", 30 de decembro 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 xaneiro 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

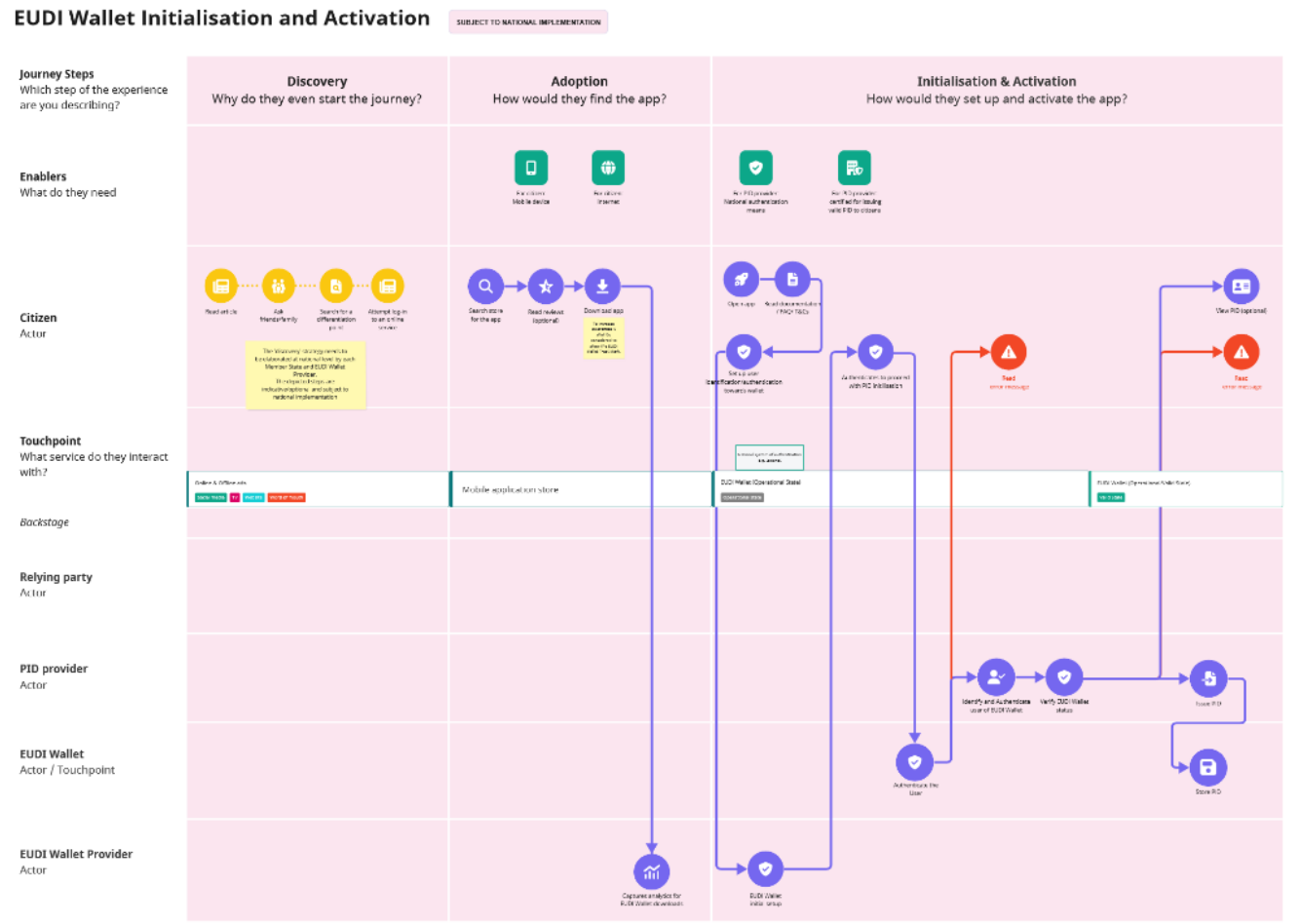
[JOSE] RFC7515 https://www.rfc-editor.org/rfc/rfc7515.html,
RFC7516 https://www.rfc-editor.org/rfc/rfc7516.html,
RFC7517 https://www.rfc-editor.org/rfc/rfc7517.html,
RFC7518 https://www.rfc-editor.org/rfc/rfc7518.html

[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/

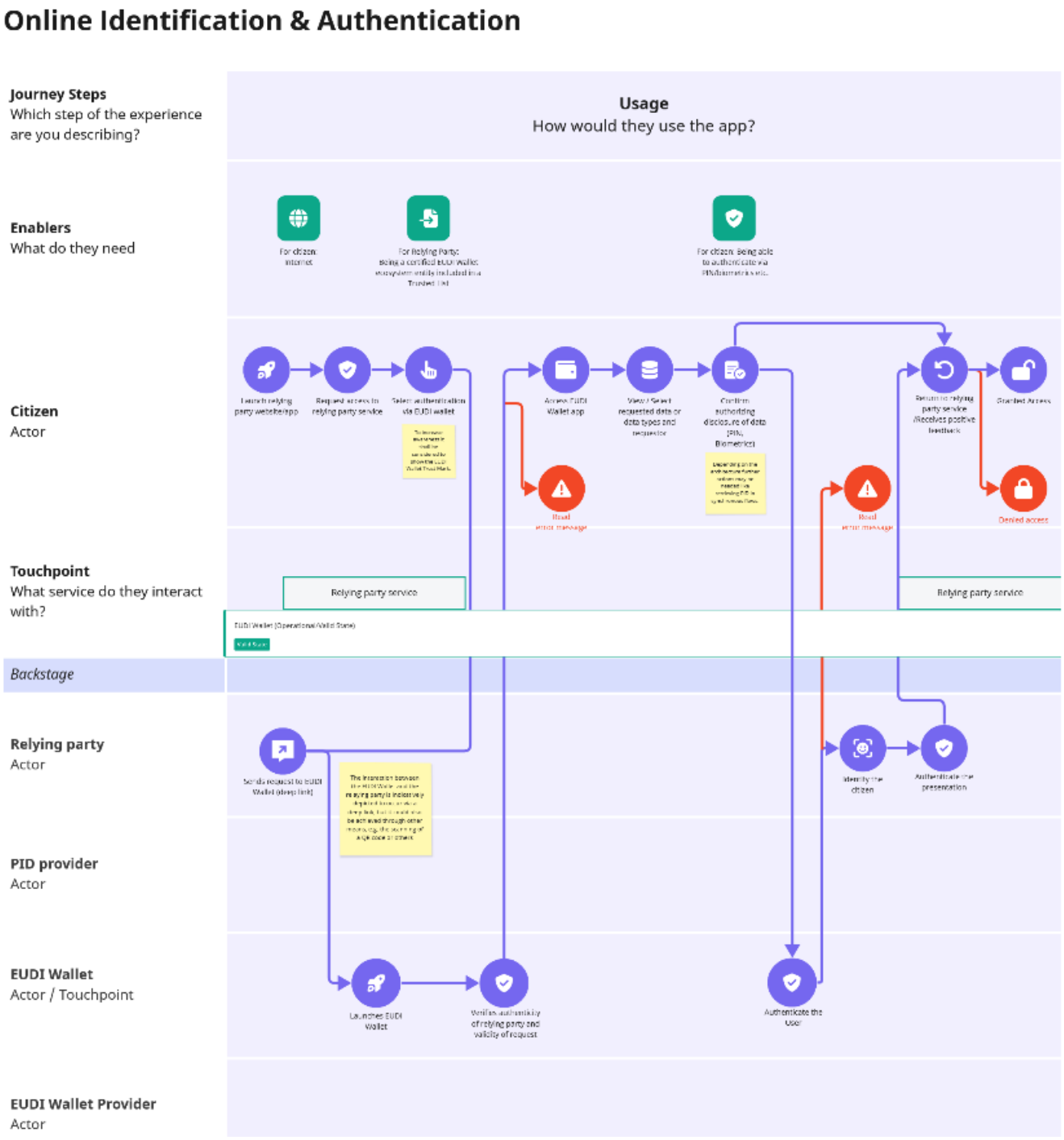
Anexo 01 - inicialización e activación

O modelo de servizo sobre a inicialización e activación da Carteira descríbese no arquivo adxunto ***Anexo 01- EUDI Wallet - Initialisation and Activation.pdf***



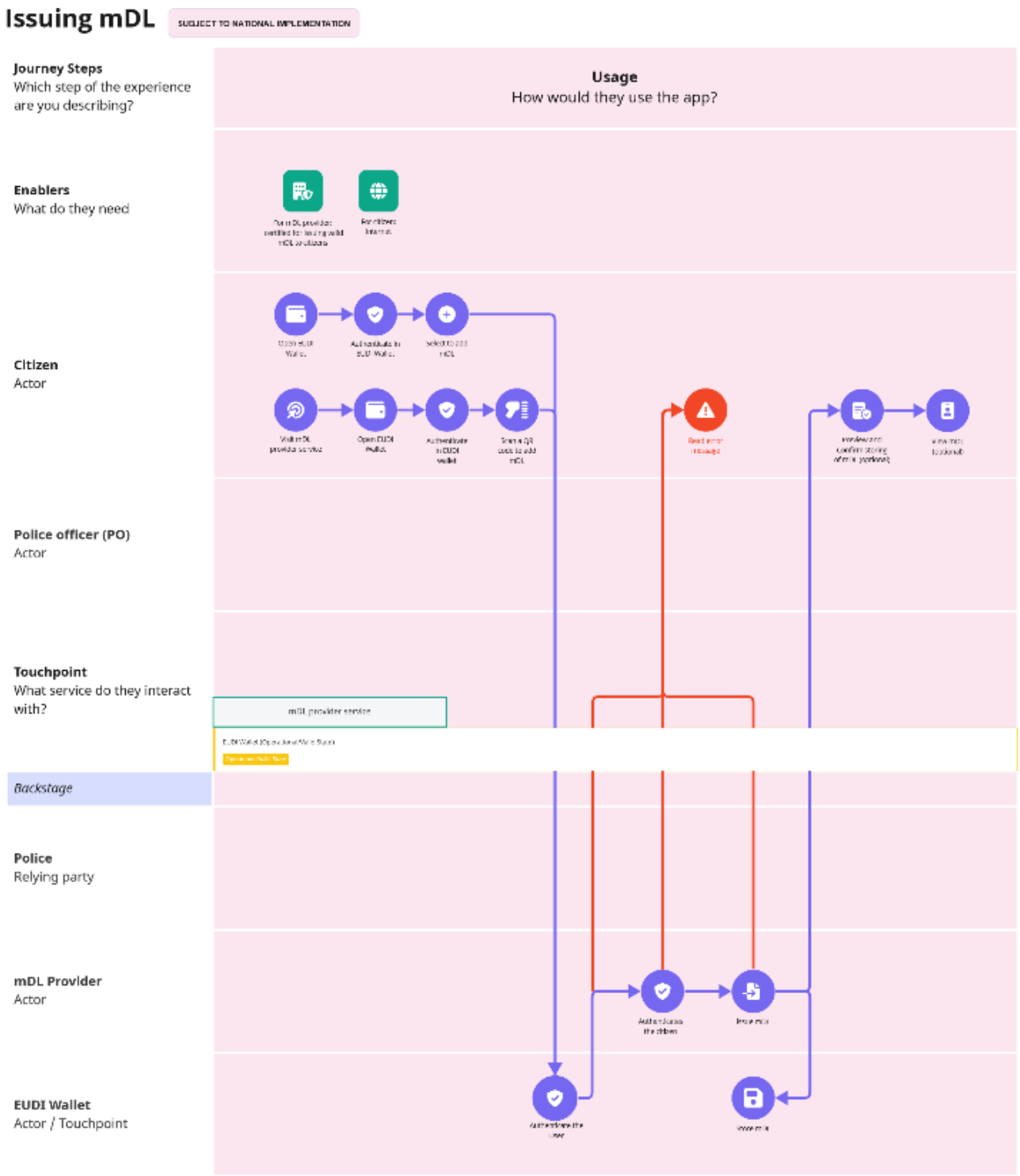
Anexo 02 - identificación e autenticación en liña

O modelo de servizo sobre identificación e autenticación en liña para a Carteira descríbese no arquivo adxunto ***Anexo 02- EUDI Wallet - Online Identification and Authentication.pdf***



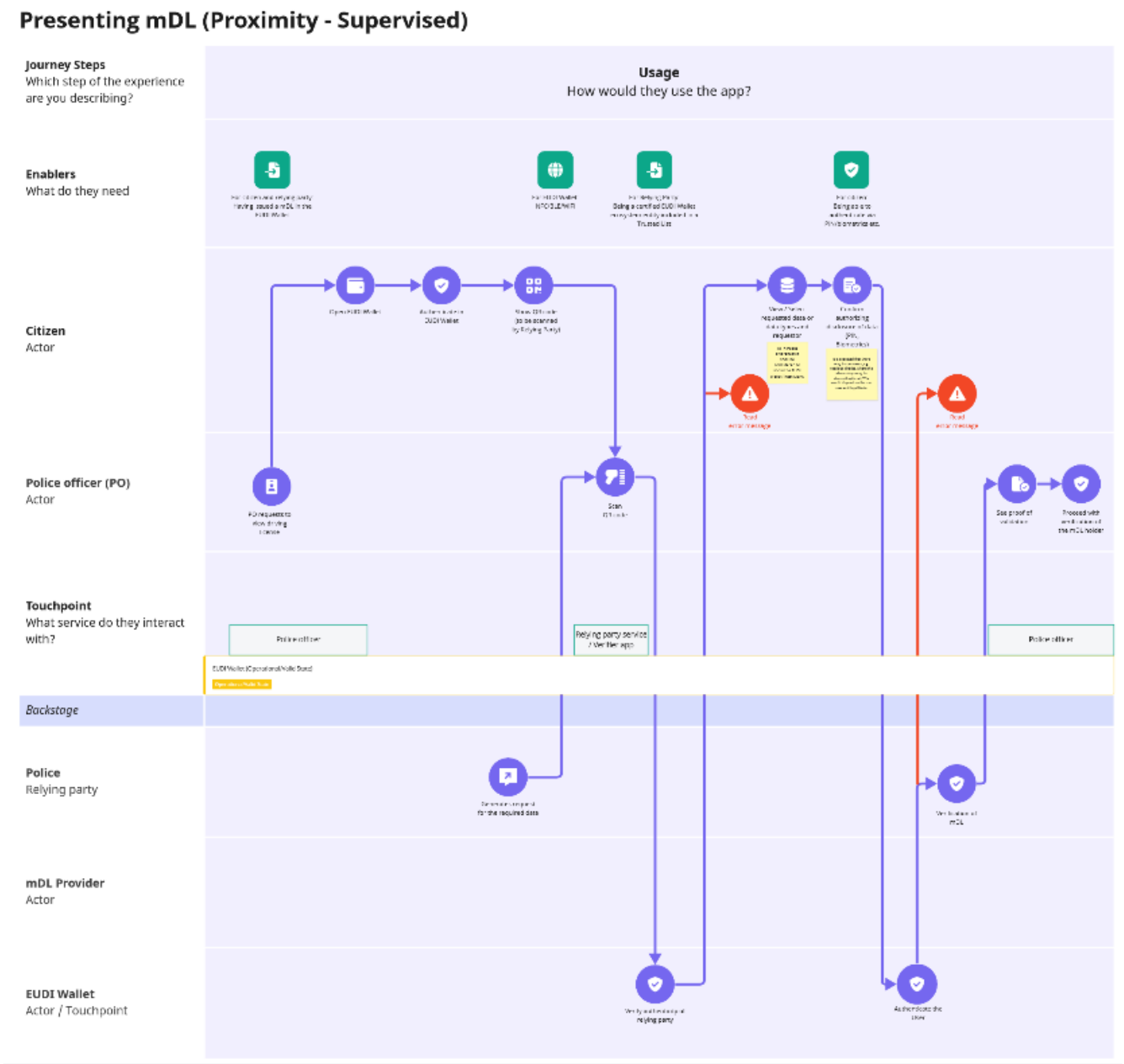
Anexo 03 - Expedición de mDL

O proxecto de servizo sobre a emisión de mDL descríbese no arquivo adxunto ***Anexo 03 - EUDI Wallet - issuing mDL.pdf***.



Anexo 04 - presentación de mDL (proximitysupervised)

O proxecto de servizo sobre a presentación ***de mDL (proximidade supervisada***) descríbese no arquivo adxunto ***Anexo 04 - EUDI Wallet - presenting mDL (proximity-supervised).pdf***.



Anexo 05 - presentación de mDL (proximityunsupervised)

O proxecto de servizo sobre a presentación ***de mDL (proximidade-sen supervisión***) descríbese no arquivo adxunto ***Anexo 05 - EUDI Wallet - presenting mDL (proximity-unsupervised).pdf***.