La Caixa d' eines
Comú de la Unió per a un enfocament coordinat cap a un Marc Europeu d'Identitat Digital

Arquitectura i marc de referència de la cartera europea d' identitat digital

Abril de 2023

Versió 1.1.0

VERSIÓ DEL DOCUMENT

VERSIÓ	DATA[1]	CANVIS
1.0.0	26 de gener de 2023	Primera versió
1.1.0	20 d'abril de 2023	Addició de plànols de serveis per a casos d' ús en: - Identificació i autenticació per accedir als serveis en línia, i - permís de conducció mòbil

[1] La data d' adopció pel Grup d' Experts eIDAS

Contingut

1. Introducció 4
1.1. Context 4
1.2. Sobre aquest document 5
1.2.1. Autoria i Llicència 5
1.2.2. Traducció i Llicència. 5
1.2.3. Finalitat d' aquest document 6
1.3. Ús d'aquest document 6
1.3.1. La implementació de referència d'una cartera IDUE 6
1.3.2. Orientacions per als pilots a gran escala (Large Scale Pilots LSP) 7
2. Definicions 8
3. Casos d' ús de la cartera EUDI 11
3.1 Identificació i autenticació per accedir a serveis en línia 11
3.2 Permís de conducció mòbil 12
3.3. Altres casos d'ús 12
4. Ecosistema europeu de carteres d' identitat digital 14
4.1. Funcions en l'ecosistema 14
4.1.1. Usuaris de Cartera IDUE 15
4.1.2. Proveïdor de carteres IDUE 15
4.1.3. Proveïdors de Dades d'Identificació de la Persona (DIP/PID) 15
4.1.4. Proveïdors de Llistes de confiança 16
4.1.5. Proveïdors de Testimoni electrònic qualificat d'atributs 16
4.1.6. Proveïdors de Testimoni electrònic no qualificat d'atributs 16
4.1.7. Prestadors de Certificats Qualificats i No Qualificats per a Signatures i segells electrònics 17
4.1.8. Proveïdors d'altres serveis de confiança 17
4.1.9. Fonts autèntiques 17
4.1.10. Parts Informades (o Parts que confien) 18
4.1.11. Organismes d'avaluació de la conformitat (OEC) 18
4.1.12. Organismes de supervisió 19
4.1.13. Fabricants de dispositius i entitats relacionades 19
4.1.14. Proveïdors d'esquemes de Testimonis Electrònics d'atributs Qualificat i No qualificats 19

4.1.15. Organismes nacionals d'acreditació 19
4.2. Cicle de vida d'una cartera IDUE 20
4.2.1. Model simplificat de cartera IDUE 20
4.2.2. Cicles de vida dels DIP/PID i dels TE(C)A/(Q)EAA 21
4.2.3. Cicle de vida de la solució Cartera IDUE 22
4.2.4. Cicle de vida de la instància de cartera IDUE 23
5. Requisits per a l'expedició de DIP/PID i TE(C)A/(Q)EAA 25
5.1. Dades d'identificació de la persona 25
5.1.1 El conjunt de dades 25
5.1.2 Requisits d' expedició de l' EPI 26
5.2. Testimoni electrònic d'atribut qualificat i no qualificat 28
5.2.1 Requisits d' expedició dels TE(C) A/(Q) EAA 28
6. Arquitectura de referència i fluxos 30
6.1. Consideracions sobre el disseny 30
6.2. Components d'arquitectura 30
6.3. Arquitectura lògica 32
6.4. Tipus de fluxos 34
6.5. Configuracions de la cartera 36
6.5.1. Justificació 36
6.5.2. Configuracions inicials 36
6.5.3. Requisits de configuració 37
7. El procés de certificació de les carteres IDUE 41
8. Procés de desenvolupament de l' Arquitectura i del Marc de referència 42
8.1. Publicació 42
8.2. Actualització 42
8.2.1. Versions de documents 43
9. Referències 44
Annex 01 - inicialització i activació 45
Annex 02 - identificació i autenticació en línia 46
Annex 03 - Expedició de mDL 47
Annex 04 - presentació de mDL (proximitysupervised) 48
Annex 05 - presentació de mDL (proximityunsupervised) 49

1. Introducció

1.1. Context

El 3 de juny de 2021, la Comissió Europea va adoptar una Recomanació[2] en la qual es demana als Estats membres que treballin en el desenvolupament d'una caixa d'eines que inclogui una arquitectura tècnica i un marc de referència (en endavant, l'ARF, per la seva designació en anglès "Architecture and Reference Framework"), un conjunt de normes comunes i especificacions tècniques i un conjunt de directrius comunes i millors pràctiques.

La Recomanació especifica que aquests resultats serviran de base per a l' aplicació de la proposta de Marc Europeu d' Identitat Digital[3] sense que el procés d' elaboració de la caixa d' eines interfereixi o prejutgi el procés legislatiu.

La Recomanació preveu que la caixa d'eines sigui desenvolupada per experts dels Estats membres en el Grup d'Experts eIDAS[4]en estreta coordinació amb la Comissió i, quan sigui pertinent per al funcionament de la infraestructura de la Cartera d'Identitat Digital de la Unió Europea (IDUE), amb altres parts interessades dels sectors públic i privat.

Seguint el calendari indicatiu establert en la Recomanació, el 30 de setembre de 2021 es van acordar un procés i uns procediments de treball que es van debatre en un document oficiós sobre una descripció d'alt nivell de l'ecosistema Cartera IDUE, proposat per la Comissió.

Sobre aquesta base, entre octubre i desembre de 2021 es va definir un esquema que proporcionava una descripció més detallada del concepte de cartera IDUE, les seves funcionalitats i aspectes de seguretat, així com de diversos casos d'ús bàsics. Aquest treball va donar lloc a l'Esbós de l'ARF, adoptat pel Grup d'Experts eIDAS el febrer de 2022. L'esquema es va publicar a Futurium[5] per recaptar l'opinió del públic. Quan es va tancar el període de comentaris el 15 d'abril de 2022, 36 parts interessades havien enviat els seus comentaris sobre l'Esbós.

Des d' aleshores, el Grup d' Experts eIDAS ha seguit desenvolupant els conceptes i especificacions del Marc Europeu d' Identitat Digital sobre la base de la proposta de revisió del

[2] RECOMANACIÓ DE LA COMISSIÓ (UE) C(2021) 3968 final de 3 de juny de 2021 sobre una caixa d'eines comuna de la Unió per a un enfocament coordinat cap a un marc europeu d'identitat digital, DO L 210/51 de 14.6.2021.

[3] Totes les referències en el document a la revisió del Reglament eIDAS s' han d' entendre fetes a la proposta de la Comissió de 3 de juny de 2021, llevat d' indicació en contrari. Proposta de REGLAMENT DEL PARLAMENT EUROPEU I DEL CONSELL pel qual es modifica el Reglament (UE) nº 910/2014 pel que fa a l'establiment d'un marc per a la identitat digital europea, COM(2021) 281 final de 3.6.2021

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

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

Reglament EIDAS de la Comissió[6] i seguirà fent-ho fins que concloguin les negociacions legislatives i s' adoptin els actes d' execució.

El Grup d'Experts eIDAS va adoptar el present document el 20 d'abril de 2023.

1.2. Sobre aquest document

1.2.1. Autoria i Llicència

Aquest document és el resultat del treball del Grup d'Experts eIDAS (eIDAS Expert Group) (E03032)[7] l'última reunió del qual va tenir lloc el 20/03/2023 (als efectes d'aquesta versió del document).

La versió original en anglès d' aquest document mantinguda en una eina que promou la cooperació i contribucions de diferents autors està disponible en https://code.europa.eu/eudi/architecture-and-reference-framework

Aquesta forma de gestionar el document fa recomanable recórrer a aquesta URL per accedir a les versions més actualitzades del document en anglès.

1.2.2. Traducció i Llicència.

La versió en espanyol l'ha realitzat **Julián Inza**, President d'EADTRUST, un Prestador Qualificat de Serveis de Confiança radicat a Madrid (Espanya) amb pàgina web https://eadtrust.eu i s'ha finalitzat l'11 de setembre de 2023, diverses setmanes dies després que es publiqués la versió

[6] Totes les referències del document a la revisió del Reglament eIDAS s' han d' entendre fetes a la proposta de la Comissió de 3 de juny de 2021, llevat que s' indiqui el contrari.
[7] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3032

original en anglès a la pàgina web de Github https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

Qualsevol obra derivada ha d'indicar que s'ha desenvolupat a partir de la traducció realitzada per **Julián Inza**, President d'EADTRUST European Agency of Digital Trust, S.L, un Prestador Qualificat de Serveis de Confiança radicat a Madrid (Espanya) amb pàgina web https://eadtrust.eu

1.2.3. Finalitat d' aquest document.

L' objectiu del document és proporcionar totes les especificacions necessàries per desenvolupar una solució interoperable de cartera IDUE basada en normes i pràctiques comunes. El document presenta un estat dels treballs en curs del Grup d' Experts eIDAS i no implica cap acord formal sobre el seu contingut o la proposta de revisió del Reglament EIDAS. Aquest document es complementarà i actualitzarà amb el temps a través del procés de creació de la caixa d' eines, tal com es descriu en el capítol 8. Una vegada completat, el document descriurà una Arquitectura i un Marc de Referència complets que abastaran totes les especificacions necessàries per implantar una Solució Europea de Cartera d'Identitat Digital.

Mentre que els capítols 2-4 i 7-8 són descriptius, els capítols 5 i 6 especifiquen els requisits per als prestadors de DIP/PID i TE(C)A/(Q)EAA i els implementadors de solucions de Cartera IDUE. Les expressions imperatives en majúscules en el document s' utilitzen d' acord amb la norma tècnica RFC 2119.

El document en si no té valor legal i no prejutjarà el procés legislatiu en curs i els requisits legals obligatoris finals per a les carteres europees d'identitat digital. L' ARF s' ajustarà al resultat de les negociacions legislatives de la proposta de Marc Europeu d' Identitat Digital. Només seran obligatoris el Reglament Marc Europeu d' Identitat Digital finalment adoptat i els actes d' execució i delegats adoptats d' acord amb aquesta base jurídica.

1.3. Ús d'aquest document

Aquest document està destinat principalment a ser utilitzat per la Comissió Europea que desenvolupa una implementació de referència d'una Cartera IDUE i els consorcis que executen projectes pilot enfocats en l'ús de la implementació de referència en el context de "Large Scale Pilots" (Pilots a Gran Escala). L' experiència adquirida en l' aplicació d' aquesta especificació pot donar lloc a millores del present document, de conformitat amb el capítol 8.

1.3.1. La implementació de referència d'una cartera IDUE

La Comissió proporcionarà una implementació de referència de la cartera IDUE en un format mòbil[8]. El codi de la implementació de referència de Cartera IDUE es proporcionarà com a programari de fonts obertes per a la seva reutilització pels implementadors de tot Europa. Els primers implementadors seran els projectes seleccionats per dur a terme els Large Scale Pilots (LSPs), després d'una convocatòria de propostes semblant a una licitació. Els projectes LSP participaran en el desenvolupament de la implementació de referència d' una Cartera IDUE. La Comissió també prestarà inicialment els serveis centrals necessaris per al funcionament de la implementació de referència de la Cartera IDUE.

La Comissió es proposa utilitzar l' ARF per desenvolupar l' aplicació de referència de la Cartera IDUE.

1.3.2. Orientacions per als pilots a gran escala (Large Scale Pilots LSP)

Per donar suport al desenvolupament d'una implementació de referència d'una cartera IDUE i provar el seu ús a través de diferents casos d'ús prioritaris en projectes pilot, la Comissió va llançar una convocatòria de propostes el 22 de febrer de 2022 en el marc del Programa Europa Digital per acollir casos d'ús a gran escala per a la cartera IDUE.

L'objectiu de la convocatòria Large Scale Pilots (LSP) és cofinançar projectes pilot que facin ús de la cartera IDUE basada en una implementació de referència del programari de cartera IDUE, tenint en compte les especificitats del projecte, els sistemes existents d'Identitat Digital notificats (com el DNI en el cas d'Espanya) i els desenvolupaments nacionals de sistemes de Cartera i les situacions d'implementació, al voltant dels diferents casos d' ús transfronterers que impliquen parts interessades tant públiques com privades.

L' ARF serà utilitzat pels LSP per informar i guiar el disseny de sistemes dels pilots i el desenvolupament de l' arquitectura juntament amb la publicació de la implementació de referència.

S'espera que els LSP aportin els seus comentaris sobre l'ARF a mesura que desenvolupin i interactuïn amb els serveis de les parts de confiança, els proveïdors qualificats o no qualificats de testimonis electrònics d'atributs TE(C)A/(Q)EAA, els proveïdors de dades d'identificació de persones (DIP/PID) i els usuaris en transaccions significatives segons els casos d'ús proposats.

[8] Actualment està prevista una primera versió per al segon trimestre de 2023, a la qual seguiran altres.

2. Definicions

A més de l'article 3 de la proposta de modificació del text legal del Reglament EIDAS (anterior Reglament UE 910/2014) s'ofereixen les següents definicions per a destacar les més rellevants per a l'Arquitectura i el Marc de Referència o per a introduir termes addicionals no definits en l'esmentat text legal (assenyalats amb un *).

Atribut	**Tret, característica o qualitat d'una persona física o jurídica o d'una entitat, en forma electrònica. - *Proposta de modificació del Reglament eIDAS***
Font autèntica	**Repositori o sistema, mantingut sota la responsabilitat d'un organisme del sector públic o una entitat privada, que conté atributs sobre una persona física o jurídica i es considera la font primària d'aquesta informació o es reconeix com a autèntica en la legislació nacional. - *Proposta de modificació del Reglament eIDAS***
Testimoni electrònic d'atributs (TEA)	*En anglès: Electronic Attestation of Attributes (EAA)* **Un testimoni en format electrònic que permet l'autenticació d'atributs - *Proposta de modificació del Reglament eIDAS***
*Emissor**	**Un prestador que informa sobre dades d'identificació de persona (DIP/PID) o un prestador de serveis de confiança (qualificat o no) que emet atributs TE(C)A/(Q)EAA. En el cas de la cartera IDUE, hi pot haver diversos emissors de DIP/PID i de TE(C)A/(Q)EAA.**
Organismes nacionals d'acreditació (ONA).*	*En anglès: National Accreditation Bodies (NAB)* **Els Organismes Nacionals d'Acreditació (ONA) d'acord amb el Reglament (CE) nº 765/2008 són els organismes dels Estats membres que realitzen l'acreditació d'Organismes d'Avaluació de Conformaitat amb autoritat derivada de l'Estat.**
Dades d'identificació de la persona (DIP)	*En anglès: Person Identification Data (PID)* **Conjunt de dades que permeten establir la identitat d'una persona física o jurídica, o d'una persona física que representa una persona jurídica - *Reglament eIDAS*.**
*Proveïdor de dades d' identificació de persones**	**Estat membre o entitat jurídica que proporciona dades d' identificació de la persona als usuaris com a font primària.**
Infraestructura de clau pública (PKI).*	*En anglès, Public Key Infraestructure (PKI)* **Denota sistemes, programari i protocols de comunicació que utilitzen els components d' una Cartera IDUE per distribuir,**

	gestionar i controlar claus públiques. Una PKI lliura claus públiques embegudes en certificats i gestiona la seva confiabilitat responent sobre la vigència dels certificats que ha emès.
Prestador de Testimonis electrònics qualificades d' atributs	**Proveïdor qualificat de serveis de confiança que expedeix testimonis electrònics d'atributs, i que compleix els requisits establerts a l'annex V. - *Proposta de modificació del Reglament eIDAS***
Dispositiu Qualificat de Creació de Signatura (DCCF)	*En anglès, Qualified Signature creation Device (QSCD)* **Programari o maquinari configurat per crear signatures electròniques que compleixi els requisits establerts a l' annex II de la proposta de modificació del Reglament eIDAS. *Reglament eIDAS i proposta de modificació del Reglament eIDAS***
Prestador qualificat de serveis de confiança (PCSC)	*En anglès, Qualified Trust Service Provider (PCSC)* **Un proveïdor de serveis de confiança que presta un o diversos serveis de confiança qualificats quan l' organisme de supervisió li hagi concedit la condició de qualificat. - *Reglament eIDAS***
Part que confia Part informada*	**Persona física o jurídica que confia en una identificació electrònica o en un servei de confiança. - *Reglament eIDAS*** **En el cas de Cartera IDUE, la part que rep la informació d' identificació electrònica o d' atributs procedent de Cartera IDUE.**
Divulgació selectiva.*	**Capacitat de la cartera IDUE que permet a l'usuari presentar un subconjunt d'atributs d'entre els que figuren als DIP/PID o als TE(C)A/(Q)EAA.**
*Confiança**	**La confiança és la característica per la qual una part està disposada a confiar en una tercera entitat perquè executi una sèrie d'accions i/o realitzi una sèrie d'afirmacions sobre una sèrie de temes i/o àmbits.[9].**
*Marc de confiança**	**Conjunt jurídicament exigible de normes i acords operatius i tècnics que regeixen un sistema de múltiples intervinents dissenyat per realitzar determinats tipus de transaccions entre una comunitat de participants i subjecte a un conjunt comú de requisits.**
*Model de confiança **	**Conjunt de normes que garanteixen la legitimitat dels components i les entitats que intervenen en l' ecosistema de la Cartera IDUE.**

[9] Segons especificacions d'"OASIS Trust", [en línia]. Disponible: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html.

Proveïdor de serveis de confiança (PSC)	*En anglès, Trust Service Provider (TSP)* **Persona física o jurídica que presta un o diversos Serveis de confiança, ja sigui com a Prestador de Serveis de confiança qualificat o com a Prestador de Serveis de confiança no qualificat. - *Reglament eIDAS***
Servei de confiança	**Un servei electrònic prestat normalment previ pagament que consisteix en:** **(a) la creació, verificació i validació de certificats electrònics que donen suport a signatures electròniques i segells electrònics, l'emissió de segells de temps electrònics, la prestació de serveis de lliurament electrònic certificat i la prestació de serveis de testimoni electrònic d'atributs;** **(b) la creació, verificació i validació de certificats per a l'autenticació de llocs web;** **(c) la conservació de documents electrònics que inclouen signatures electròniques o segells electrònics;** **(d) l'arxiu electrònic de documents electrònics;** **(e) la gestió de dispositius remots de creació de firmes i segells electrònics, sota control del seu titular, securitzant l'ús de claus privades i certificats;** **(f) el registre de dades electrònices en un llibre diari de moviments semblant a un registre de comptabilitat electrònic. - *Proposta de modificació del Reglament eIDAS***
*Llista de confiança**	**Repositori d' informació sobre entitats dotades d' autoritat en un determinat context legal o contractual que proporciona informació sobre el seu estat actual i històric. Les llistes de confiança es poden implementar de diferents maneres.**
*Usuari**	**És una persona física o jurídica que utilitza una Cartera IDUE.**
*Instància de cartera IDUE**	**Instància d' una Solució de Cartera IDUE pertanyent a un Usuari i que està sota el seu control.**
*Proveïdors de carteres IDUE**	**Organització, pública o privada, responsable del funcionament d'una solució de cartera IDUE compatible amb eIDAS que es pot fer, per exemple, mitjançant la seva instal·lació i inicialització.**
Solució Cartera IDUE.*	**Una solució de cartera IDUE és el conjunt de productes i serveis complet propietat d' un proveïdor de carteres IDUE, ofert a tots els usuaris d' aquesta solució. Una solució Cartera IDUE pot ser certificada com a conforme amb IDUE per un CAB.**

Quadre 1. Definicions

** Addicional a les definicions de l' article 3 del Reglament eIDAS o la seva proposta de modificació.*

3. Casos d' ús de la cartera EUDI

El desenvolupament de les especificacions de Cartera IDUE (EUDI Wallet) es regeix per casos d'ús que faciliten la comprensió de l'experiència de l'usuari alhora que capten la proposta de valor i els requisits empresarials de la Cartera IDUE. Per a això, el Grup d'Experts d'eIDAS comença creant models de servei per a cada cas d'ús de la Cartera IDUE. Aquests esquemes són representacions visuals dels diferents components i processos que intervenen en la prestació d' un servei als usuaris i serveixen com a eina per identificar possibles àrees de millora, optimitzar l' experiència de l' usuari i agilitar la prestació del servei. Aquests esquemes serveixen de base per establir regles d' ús i especificacions comunes per a tots els casos d' ús.

Els esquemes de servei del cas d' ús es troben als annexos com a documents adjunts. És important assenyalar que els esquemes de servei ofereixen una solució viable per a cada cas d' ús, però existeixen alternatives i passos opcionals. Per exemple, mostrar dades emmagatzemades per a les quals l'usuari ja ha donat el seu consentiment pot ser opcional. A més, els recorreguts de l'usuari (user journeys) poden variar en funció de l'enfocament d'implementació triat, com l'emmagatzematge asíncron d'atributs o la recuperació síncrona. Això podria afectar aspectes com la prestació del consentiment per recuperar i compartir dades.

El Grup d' Experts eIDAS ha descrit esquemes de servei per als següents casos d' ús.

3.1 Identificació i autenticació per accedir a serveis en línia

L'objectiu principal de la Cartera IDUE és oferir una identificació i autenticació segures dels usuaris amb un alt Nivell d'Assegurament (Level of Assurance, LoA) per als serveis en línia públics i privats. Aquesta funcionalitat essencial garanteix que les Parts Informades puguin verificar amb seguretat que estan interactuant amb la persona correcta.

En aquest cas, l'usuari utilitza la Cartera IDUE per confirmar la seva identitat. Accedeix amb freqüència a serveis en línia que exigeixen autenticació i actualment empra diversos mètodes per verificar la seva identitat en accedir a aquests serveis. A l'usuari també li preocupa compartir dades d'identificació personal (PID) durant les interaccions en línia. Els seus objectius inclouen identificar-se amb serveis que requereixen la identificació de l' usuari i mantenir el control sobre l' intercanvi de dades personals.

Aquest cas d' ús abasta tot el cicle de vida de la Cartera IDUE des del punt de vista de l' usuari, des de l' obtenció d' una Cartera vàlida fins a la identificació i autenticació de l' usuari dins d' un servei en línia. La descripció actual se centra en un flux remot viable del mateix dispositiu (vegeu la secció 6.4), en el qual un Usuari persona física empra un únic dispositiu mòbil tant per securitzar la sessió com per accedir a la informació del servei.

3.2 Permís de conducció mòbil

Un cas d'ús significatiu per a la Cartera IDUE consisteix a permetre als usuaris adquirir, emmagatzemar i mostrar un document digital com el carnet de conduir mòbil (movile Driving License, mDL) per demostrar la seva habilitació per conduir. En aquest cas, l'usuari utilitza la Cartera IDUE per presentar el permís a un tercer, com un agent de policia.

La descripció del cas d'ús se centra en els fluxos de proximitat supervisats i no supervisats, que impliquen escenaris en els quals l'usuari es troba físicament prop d'una Part Informada, i l'intercanvi i divulgació d'atributs mDL es produeix utilitzant tecnologies de proximitat (per exemple, NFC, Bluetooth). Els dos fluxos de proximitat tenen una diferència significativa: en el flux *supervisat*, la Cartera IDUE presenta els atributs mDL a una Part Informada humana o sota la seva supervisió (amb ajuda d'un dispositiu); mentre que, en el flux *no supervisat*, la Cartera IDUE presenta els atributs mDL a una màquina sense supervisió humana.

3.3. Altres casos d'ús

En versions posteriors d' aquest document, els següents casos d' ús es detallaran com a models de servei:

- *Salut*

El fàcil accés a les dades sanitàries és crucial tant en contextos nacionals com transfronterers. La Cartera IDUE pot permetre l' accés a la fitxa del pacient, receptes electròniques, etc.

- *Formació i qualificacions professionals*

Facilitar documents per als procediments de convalidació de qualificacions pot resultar costós i portar molt de temps als usuaris finals, empreses i ocupadors, proveïdors d' educació i formació i altres institucions acadèmiques. Per exemple, els testimonis digitals de diplomes es podrien presentar de forma transfronterera en un format verificable, fiable i consumible a una altra institució educativa o de formació o a un possible ocupador. La cartera IDUE permet recollir credencials digitals educatives en forma de Testimonis Electrònics d'Atributs facilitant que els alumnes les recopilen i les presentin.

- *Finances digitals*

La cartera IDUE facilitarà el compliment dels requisits d' autenticació reforçada del client en entorns financers. En consonància amb l' Estratègia de Pagaments Minoristes de la Comissió[10]el cas d' ús es desenvoluparà en estreta coordinació amb els grups consultius dels Estats membres sobre pagaments minoristes i amb el sector financer.

[10] Comunicació de la Comissió al Parlament Europeu, al Consell, al Comitè Econòmic i Social Europeu i al Comitè de les Regions sobre una estratègia de pagaments minoristes per a la UE COM/2020/592 final.

- *Credencial digital de viatge*

La Cartera IDUE pot emmagatzemar credencials digitals de viatge que permeten als usuaris beneficiar-se de viatges més fluids.

Aquest treball podrà ampliar-se en el futur a altres casos d' ús.

4. Ecosistema europeu de carteres d' identitat digital

Aquest capítol descriu l'ecosistema de la Cartera IDUE tal com està previst en la proposta legislativa de la Comissió Europea per a la reforma del Reglament UE 910/2014.

4.1. Funcions en l'ecosistema

Les funcions de l' ecosistema Cartera IDUE es descriuen en la Figura 1 i es detallen en les seccions següents.

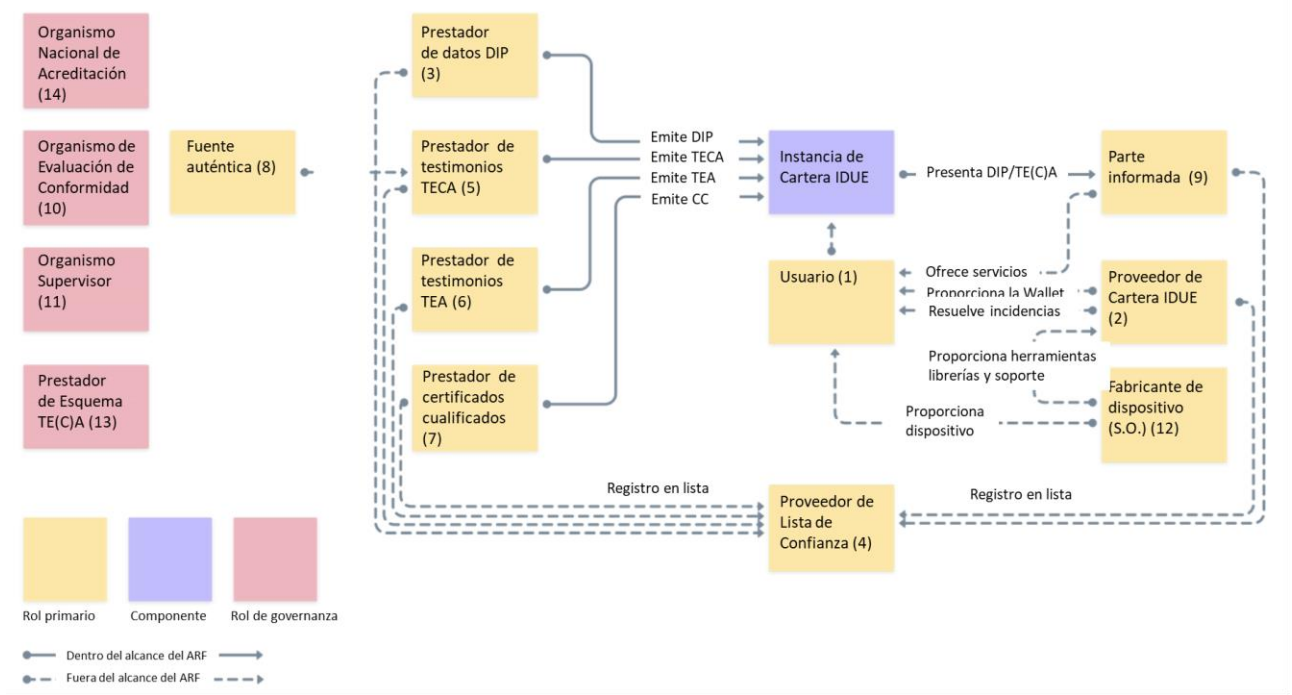


Figura 1: Visió general de les funcions de la cartera IDUE

1. *Usuaris finals de les Carteres IDUE*
2. *Proveïdors de Carteres IDUE*
3. *Proveïdors de Dades d' Identificació de Persones*
4. *Proveïdors de Llistes de Confiança*
5. *Proveïdors de testimonis electrònics qualificats d'atributs (TECA/QEAA)*
6. *Proveïdors testimonis electrònics no qualificats d'atributs (TEA/EAA)*
7. *Proveïdors qualificat o no qualificats de certificats de signatura electrònica/segell electrònic*
8. *Fonts autèntiques*
9. *Parts informades*
10. *Organismes d'Avaluació de la Conformitat (OEC)*
11. *Organismes de supervisió*
12. *Fabricants de dispositius i proveïdors de subsistemes relacionats*
13. *Proveïdors d'esquemes de testimonis TEA/EAA o TECA/QEAA*
14. *Organismes nacionals d' acreditació*

4.1.1. Usuaris de Cartera IDUE

Els usuaris de Carteres IDUE utilitzen la Cartera IDUE per rebre, emmagatzemar i presentar testimonis (DIP/PID, TECA/QEAA o TEA/EAA) sobre si mateixos, fins i tot per demostrar la seva identitat. Els usuaris poden crear Firmes i Segells Electrònics Qualificats (QES) utilitzant una Cartera IDUE.

En funció de la legislació nacional es determina qui pot ser usuari d' una cartera IDUE. L' ús d' una cartera IDUE no és obligatori per als ciutadans segons la proposta de revisió del Reglament EIDAS. No obstant això, els Estats membres estan obligats a oferir almenys una solució de cartera IDUE als seus ciutadans.

4.1.2. Proveïdor de carteres IDUE

Els proveïdors de carteres IDUE són Estats membres o organitzacions autoritzades o reconegudes pels Estats membres que posen la cartera IDUE a disposició dels usuaris finals. Correspon a cada Estat membre determinar els termes i condicions del mandat o reconeixement.

Els Proveïdors de Carteres IDUE posen a disposició dels Usuaris a través d'una Solució de Cartera IDUE una combinació de diversos productes i Serveis de Confiança previstos en la proposta de revisió del Reglament EIDAS, que donen a l'Usuari el control total sobre l'ús de les seves Dades d'Identificació de Persona (DIP/PID) i Testimonis Electrònics d'Atributs Qualificats o no Qualificats (TECA/QEAA o TEA/EAA), i qualsevol altra dada personal dins de la seva Cartera IDUE. Des d'un punt de vista tècnic, això també pot implicar garantir a l'Usuari el control exclusiu sobre el material criptogràfic sensible (per exemple, claus privades) relacionat amb l'ús d'aquestes dades en alguns escenaris, inclosa la identificació electrònica, o la realització de firmes o segells electrònics.

Els proveïdors de carteres IDUE són responsables de garantir el compliment dels requisits per a les carteres IDUE.

4.1.3. Proveïdors de Dades d'Identificació de la Persona (DIP/PID)

Els proveïdors de DIP/PID són entitats de confiança responsables de:

- verificar la identitat de l'Usuari de Cartera IDUE de conformitat amb els requisits de Nivell d'Assegurament Alt (LoA high),
- expedir DIP/PID a la Cartera IDUE en un format comú harmonitzat i
- facilitar informació[11] perquè les Parts Informades verifiquin la validesa del DIP/PID.

Correspon a cada Estat membre determinar les condicions d' aquests serveis.

Els proveïdors de DIP/PID poden ser, per exemple, les mateixes organitzacions que avui dia expedeixen documents d'identitat oficials, mitjans d'identitat electrònics, proveïdors de carteres IDUE, etc. Els proveïdors de carteres IDUE poden ser o no les mateixes organitzacions que els proveïdors de DIP/PID.

[11] Sens perjudici del mecanisme concret pel qual es faciliti la informació, ja sigui directament o indirectament

4.1.4. Proveïdors de Llistes de confiança

L' estatus específic d' un rol en l' ecosistema Cartera IDUE haurà de poder ser verificat de forma fidedigna. Aquests rols són:

- Proveïdors de carteres IDUE
- Proveïdors de Dades d' Identificació de Persones
- Proveïdors de testimonis electrònics d'atributs qualificats (TECA/QEAA)
- Proveïdors de Certificats qualificats per a signatura i segell electrònics (CC/QC)
- Parts informades (en certes ocasions, Parts que Confien)
- Proveïdors no qualificats de testimonis electrònics d'atributs (TEA/EAA)
- Proveïdors de Certificats no qualificats per a signatura i segell electrònics
- Proveïdors d' altres serveis de confiança
- Catàlegs d' atributs i Esquemes per a proveïdors de testimoni d' atributs

Altres funcions poden ser necessàries i, per tant, s' han de definir i esmentar explícitament en funció de la funció específica i de la seva criticitat, per exemple, les diferents funcions i actors implicats en els processos de signatura a distància.

Quan s' utilitza, una Llista de Confiança ha de[12] comptar amb un mecanisme que permeti incorporar o retirar informació sobre les entitats fiables de l' àmbit concret a què es refereix mantenint el registre d' aquestes entitats i proporcionant a tercers la seva informació. Correspon a cada entitat gestora d'una llista de confiança (registrador) establir les condicions que han de complir les entitats per figurar a la llista, almenys que vinguin predeterminades per una normativa ja existent, per exemple, en normativa sectorials.

4.1.5. Proveïdors de Testimoni electrònic qualificat d'atributs

Els testimonis TEA/EAA qualificats les presten els PCSC (Prestadors Qualificats de Serveis de Confiança, en anglès QTSP, Qualified Trust Service Providers). El marc de confiança general per als PCSC s'aplica també als TECA/QEAA, però també cal definir normes específiques per a aquest servei de confiança. Els proveïdors de TECA/QEAA mantenen una interfície per sol·licitar i proporcionar TECA/QEAA, inclosa una interfície d'autenticació mútua amb les carteres IDUE i, potencialment, una interfície cap a fonts autèntiques per verificar atributs. Els Proveïdors de TECA/QEAA proporcionen informació o la ubicació dels serveis que es poden utilitzar per preguntar sobre l'estat de validesa dels TECA/QEAA, sense poder rebre cap informació sobre l'ús dels testimonis. Correspon a cada PCSC determinar els termes i condicions d' aquests serveis, més enllà del que especifica el Reglament eIDAS.

4.1.6. Proveïdors de Testimoni electrònic no qualificat d'atributs

[12] Més endavant s'aportaran més precisions sobre com es podrien aplicar les llistes de confiança.

Els TEA no qualificats els poden proporcionar proveïdors de serveis de confiança qualificats o no qualificats. Tot i que estan supervisats segons el marc regulatori d' eIDAS, cal suposar que altres marcs jurídics o contractuals diferents de l' eIDAS regeixen en la seva majoria les normes de prestació, ús i reconeixement dels TEA ja existents.

Aquests altres marcs poden abastar àrees de política com els permisos de conduir, credencials educatives o pagaments digitals, tot i que també poden recórrer a proveïdors qualificats de testimoni electrònic d' atributs. Perquè s'utilitzin els TEA, els PSC/TSP ofereixen als usuaris una forma de sol·licitar i obtenir TEA, cosa que significa que han de complir tècnicament les especificacions de la interfície de Cartera IDUE. Depenent de les regles del domini, els proveïdors de TEA/EAA poden proporcionar informació sobre la validesa dels TEA/EAA, sense tenir la possibilitat de rebre cap informació sobre l'ús que la Part Informada farà dels TEA/EAA. Les condicions d' emissió dels TEA i els serveis connexos estan subjectes a normes sectorials.

Els prestadors qualificats i no qualificats de DIP/PID, TEA/EAA i TECA/QEAA també poden rebre la denominació de **Parts Informants**, per contrast amb les *parts que confien* en els testimonis que reben i es denominen també **Parts Informades**.

4.1.7. Prestadors de Certificats Qualificats i No Qualificats per a Signatures i segells electrònics

L'apartat 3 de l'article 6 bis del text anomenat "COM(2021)281 final" que conté la proposta de modificació del Reglament EIDAS exigeix que la cartera IDUE permeti a l'usuari crear signatures o segells electrònics qualificats. Aquest objectiu es pot assolir de diverses maneres:

- La cartera IDUE està certificada com a dispositiu qualificat de creació de firma o segell (DCCF o DCCS, en anglès Qualified Signature/Seal Creation Device, QSCD), o bé
- Implementa capacitats segures d'autenticació i invocació per a la realització de signatura/segell com a part d'un DCCF/QSCD local o un DCCF/QSCD remot gestionat per un PCSC/QTSP.

Les interfícies de Cartera IDUE amb els DCCF/QSCD s'ampliaran en futures versions d'aquest document ARF.

4.1.8. Proveïdors d'altres serveis de confiança

La interacció de Cartera IDUE amb proveïdors d' altres serveis de confiança qualificats o no qualificats, com els segells de temps, podrà descriure' s amb més detall en futures versions d' aquest document ARF.

4.1.9. Fonts autèntiques

Les Fonts Autèntiques són els repositoris o sistemes públics o privats reconeguts o exigits per la llei que contenen atributs sobre una persona física o jurídica. Les fonts autèntiques en l' àmbit de l' annex VI de la proposta de revisió del Reglament EIDAS són fonts d' atributs sobre direcció, edat, sexe, estat civil, composició familiar, nacionalitat, títols i llicències d' educació i formació, títols i llicències de qualificacions professionals, permisos i llicències públiques, dades financeres i empresarials. Les Fonts Autèntiques incloses en l'àmbit d'aplicació de l'Annex VI han de proporcionar interfícies als Proveïdors de TECA/QEAA per verificar l'autenticitat dels atributs esmentats, ja sigui directament o a través d'intermediaris designats reconeguts a nivell nacional. Les fonts autèntiques també poden emetre testimonis TE(C)A/(Q)EAA per si mateixes si compleixen els requisits del Reglament eIDAS. Correspon als Estats membres definir els termes i condicions per a la prestació d' aquests serveis, però d' acord amb les especificacions tècniques, normes i procediments mínims aplicables als procediments de verificació dels testimonis electrònics qualificades d' atributs.

4.1.10. Parts Informades (o Parts que confien)

Les Parts Informades són persones físiques o jurídiques que confien en una identificació electrònica o en un servei de confiança. En el context de les carteres IDUE, demanen els atributs necessaris continguts en el conjunt de dades DIP/PID, TECA/QEAA i TEA/EAA dels usuaris de carteres IDUE per confiar en la cartera IDUE, prèvia acceptació per part del propietari de la cartera (usuari) i dins dels límits de la legislació i les normes aplicables. La raó per confiar en la cartera IDUE pot ser un requisit legal, un acord contractual o la pròpia decisió de l' entitat informada. Per rebre informació d' una Cartera IDUE, les Parts Informades han de notificar a l' Estat Membre en el qual estan establertes sobre la seva intenció de rebre informació procedent de Carteres IDUE. Les Parts que confien han de mantenir una interfície amb Cartera IDUE per demanar testimonis amb autenticació mútua. Les parts Informades són responsables d'autenticar els DIP/PID i els TE(C)A/(Q)EAA.

4.1.11. Organismes d'avaluació de la conformitat (OEC)

Les carteres IDUE han d' estar certificades per organismes públics o privats acreditats designats pels Estats membres[13]. Els PCSC han de ser auditats periòdicament per organismes d'avaluació de la conformitat (OEC, en anglès, CAB, Conformity Assessment Bodies). Els OEC/CAB estan acreditats per un organisme nacional d'acreditació de conformitat amb el Reglament 765/2008 com a responsables de dur a terme les avaluacions en les quals els Estats membres hauran de basar-se abans d'expedir una Cartera IDUE o proporcionar l'estatus de "qualificat" a un Proveïdor de Serveis de Confiança. Les normes i règims utilitzats pels OEC/CAB per desenvolupar les seves tasques d'avaluació/homologació de les carteres IDUE s'especifiquen més endavant en el procés "Toolbox".

[13] Article 6 quater, apartat 3

4.1.12. Organismes de supervisió

Els Estats membres han de notificar a la Comissió Europea la designació d'organismes de supervisió la missió dels quals és supervisar els PCSC/QTSP i actuen, en cas necessari, en relació amb els proveïdors de serveis de confiança no qualificats.

4.1.13. Fabricants de dispositius i entitats relacionades

Les carteres IDUE disposaran de diverses interfícies amb els dispositius en els quals es basin, que podran tenir les següents finalitats:

- Emmagatzematge local.
- Accés a Internet en línia.
- Sensors com càmeres de smartphone, sensors infrarojos, micròfons, etc.
- Canals de comunicació offline com Bluetooth Low Energy (BLE), tecnologia "WIFI Aware", Near Field Communication (NFC).
- Emissors com pantalles, llanternes, altaveus, etc.
- Targetes intel·ligents i elements segurs (SE, component de smartphone).

Per a l' emmagatzematge segur de material criptogràfic, es pot establir una interfície amb dispositius o serveis específics. Altres entitats relacionades poden ser proveïdors de serveis, com proveïdors de serveis al núvol, proveïdors de botigues d'aplicacions App, etc.

La proposta legal de reforma del reglament EIDAS estableix restriccions (per exemple, el compliment de Nivell d'Assegurament Alt – "LoA high") respecte a quins tipus de dispositius i serveis es poden utilitzar per tal d'emetre el Cartera IDUE. De la mateixa manera, la disponibilitat, així com els termes i condicions dels proveïdors d' interfícies de dispositius i proveïdors de serveis relacionats, establiran altres restriccions per als proveïdors de carteres IDUE.

4.1.14. Proveïdors d'esquemes de Testimonis Electrònics d'atributs Qualificat i No qualificats

Els proveïdors d' esquemes TE(C)A/(Q) EAA publiquen esquemes i vocabularis que descriuen l' estructura i la semàntica dels testimonis TE(C)A/(Q) EAA. El que pot permetre a altres entitats, com les parts informades, el descobriment i validació dels TE(C)A/(Q)EAA. La Comissió Europea estableix les especificacions tècniques, normes i procediments mínims a aquest efecte. L' existència d' esquemes comuns, fins i tot per part d' organitzacions sectorials específiques, és fonamental per a l' adopció generalitzada dels TE(C) A/(Q) EAA.

4.1.15. Organismes nacionals d'acreditació

Els Organismes Nacionals d'Acreditació (ONA, en anglès NAB, National Accreditation Bodies) d'acord amb el Reglament (CE) nº 765/2008[14] són els organismes dels Estats membres que realitzen l'acreditació amb autoritat derivada de l'Estat membre. Els ONA/NAB acrediten els OEC/CAB com a organismes de certificació professional competents, independents i supervisats encarregats de certificar productes/serveis/processos fent ús de document(s) normatiu(s) que estableixen els requisits (per exemple, legislacions, especificacions, perfils de protecció, normes tècniques). Els ONA/NAB supervisen els OEC/CAB als quals han expedit un certificat d'acreditació.

4.2. Cicle de vida d'una cartera IDUE

El text de proposta de reforma del Reglament EIDAS defineix la cartera IDUE amb un alt nivell d'abstracció, així com als proveïdors de carteres IDUE que tenen l'obligació legal de garantir que els habitants/residents d'un Estat membre puguin obtenir una cartera IDUE vàlid i plenament funcional. El cicle de vida d' una Cartera IDUE tindrà algunes interaccions amb els Proveïdors de Llistes de Confiança que especifiquen l' estat d' un rol en l' ecosistema de Carteres IDUE d' una manera fiable. Desenvolupar una Arquitectura i un Marc de Referència que han de servir de guia per al desenvolupament d' aquesta Cartera IDUE requereix un nivell d' abstracció més detallat per ser eficient i produir una descripció de l' arquitectura prou expressiva com per ser prescriptiva.

Aquest capítol parteix d'un model d'objectes mínim i defineix el cicle de vida dels conceptes centrals: Solució de Cartera IDUE, DIP/PID, TE(C)A/(Q)EAA i Instància de Cartera IDUE. Aquests conceptes s' han triat com a punt de partida perquè el desenvolupament conjunt de l' ARF va mostrar que els cicles de vida d' aquests conceptes estan estretament entrellaçats, la qual cosa va portar a una descripció poc clara i, en conseqüència, va provocar malentesos.

El model d' objectes s' ampliarà segons sigui necessari en futures versions de l' ARF.

4.2.1. Model simplificat de cartera IDUE

En la Figura 2 es distingeixen els conceptes de Solució de Cartera IDUE i Instància de Cartera IDUE. Una Solució Cartera IDUE és el producte i/o servei complet proporcionat per un Proveïdor de Cartera IDUE. Una Instància de Cartera IDUE és una instància personal d'una Solució Cartera IDUE que s'executa en un dispositiu de l'usuari al qual pertany i que és qui la controla.

[14] Reglament (CE) nº 765/2008 del Parlament Europeu i del Consell, de 9 de juliol de 2008, pel qual s'estableixen els requisits d'acreditació i vigilància del mercat relatius a la comercialització dels productes i pel qual es deroga el Reglament (CEE) nº 339/93.

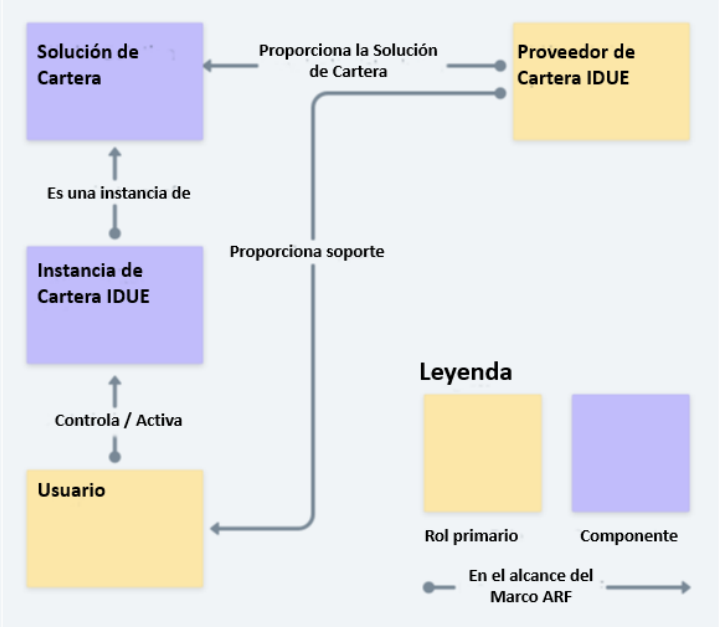


Figura 2: Model simplificat d' objectes de cartera IDUE

Aquesta definició no és prescriptiva del factor de forma, per la qual cosa, depenent de la implementació, una Instància de Cartera IDUE pot consistir en una única aplicació mòbil, o en un conjunt de components locals i remots disponibles per a un Usuari específic.

4.2.2. Cicles de vida dels DIP/PID i dels TE(C)A/(Q)EAA

Els cicles de vida dels DIP/PID i dels TE(C)A/(Q)EAA són essencialment idèntics, però, per a l'abast d'aquesta descripció ens referirem posteriorment només a l'EPI. El text d' aquesta secció aplicat a l' EPI s' aplica mutatis mutandis als TE(C) A/(Q) EAA.

El DIP/PID en el context de la Cartera IDUE comença el seu cicle de vida quan s'emet a una Instància de Cartera IDUE. Tingui en compte que això significa que la gestió d'atributs en la font autèntica (respectant les estructures nacionals i les definicions d'atributs) queda fora de l'àmbit de l'ARF.

Cal tenir en compte que, per a determinats casos d'ús, els DIP/PID poden estar preaprovisionats, cosa que significa que encara no són vàlids quan s'emeten, però assoleixen la seva validesa més tard. Si els DIP/PID s'emeten en la data d'inici de validesa o després, es considera immediatament que l'estat canvia directament a vàlid si la data de comprovació és posterior a la d'inici de validesa. Això significa que els DIP/PID podrien estar "preemesos".

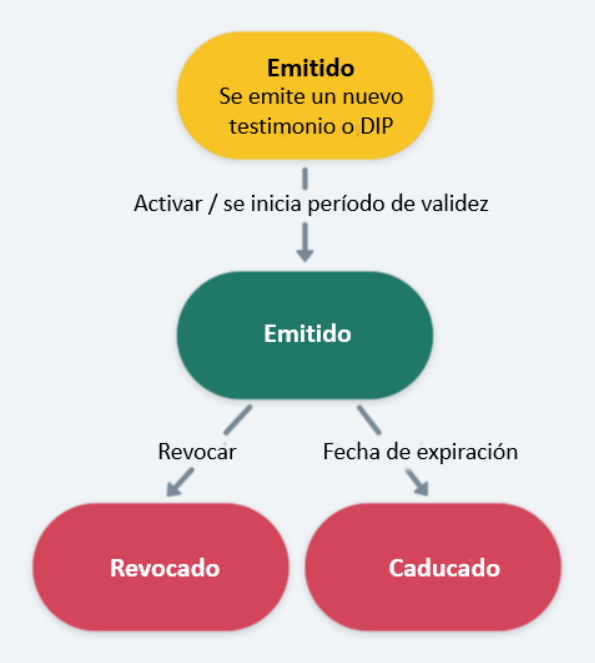


Figura 3: Diagrama d'estats del DIP/PID

Existeixen dues transicions possibles d'un DIP/PID vàlid: o bé expira automàticament, per superar-se la *"data de fi de validesa*", o bé és revocat activament pel seu Proveïdor abans de la seva expiració. L' expiració i la revocació són transicions essencialment independents. Un cop el DIP/PID ha caducat o s'ha revocat, no pot tornar a ser vàlid. L'actualització del DIP/PID (per exemple, a causa d'un canvi de nom) sempre requereix una nova emissió.

4.2.3. Cicle de vida de la solució Cartera IDUE

Una Solució Cartera IDUE té un estat propi, tal com es defineix a l' article 10 bis del futur Reglament. L' estat de la Solució afecta l' estat de totes les Instàncies de Cartera IDUE de l' esmentada Solució de Cartera IDUE. L'estat "**Candidat**" és el primer estat d'una Solució Cartera IDUE. Això significa que està totalment implementada i que el Proveïdor de Carteres IDUE demana que la solució se certifiqui com a Cartera IDUE.

Si s'han complert tots els criteris legals i tècnics, inclosa la certificació de la Solució Cartera/Wallet per l'OEC/CAB, llavors un Estat membre pot decidir començar a proporcionar **Instàncies** de la Solució als Usuaris. L'estat de la Solució passa a ser "**vàlid**". De conformitat amb l'article 6 quinquies, l'Estat membre informarà la Comissió de qualsevol canvi en l'estat de certificació de la seva Solució Cartera/Wallet. Això significa que la solució Cartera IDUE es pot llançar **oficialment** i que es poden proporcionar instàncies de la solució als usuaris.

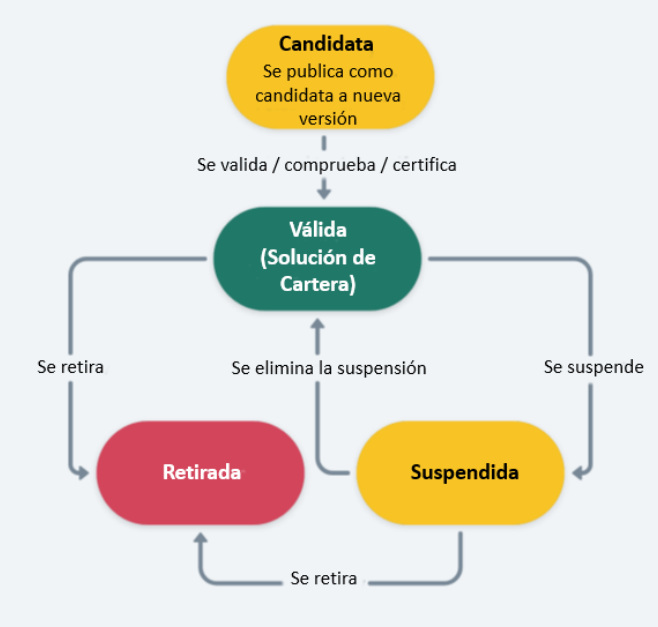


Figura 4: Diagrama d'estat de la solució Cartera/Wallet

En les condicions legals de l' article 10 bis, apartat 1, l' Estat membre emissor pot suspendre temporalment una Solució Cartera IDUE. Això podria ser, per exemple, com a conseqüència d'un problema crític de seguretat en aquesta Solució Cartera IDUE. Això dóna lloc a l'estat de "**suspesa**". De conformitat amb l'apartat 2 de l'article 10 bis, l'Estat membre emissor pot cancel·lar la suspensió de la Solució Cartera/Wallet i continuar amb l'emissió, retornant la Solució a l'estat "**vàlid**". De conformitat amb l' apartat 3, la solució Cartera IDUE pot retirar-se i cancel·lar-se per complet.

4.2.4. Cicle de vida de la instància de cartera IDUE

Una Instància de Cartera IDUE comença la seva vida basant-se en una Solució de Cartera IDUE vàlida. El Proveïdor de Cartera IDUE proporciona una Solució de Cartera IDUE a l'Usuari que es considera que executa una Instància de Cartera en estat "**operatiu**" una vegada instal·lada i activada per l'Usuari en el seu dispositiu. Depenent del factor de forma i de la implementació, proporcionar una instància pot requerir diverses accions, per exemple, instal·lació i inicialització en el cas d'una Cartera IDUE mòbil. Una Instància de Cartera IDUE d'aquest tipus podria utilitzar-se ja per a funcions no específiques d'IDUE, com emmagatzemar targetes de fidelitat o bitllets de tren no personalitzats o qualsevol altre certificat que no exigeixi la vinculació a uns DIP/PID vàlids.

Una vegada que s'inicialitza una Instància de Cartera IDUE, es considera "**vàlida**", la qual cosa significa que és reconeguda per un Proveïdor de DIP/PID i que posseeix un conjunt de DIP/PID vàlids. Si els DIP/PID caduquen o es revoquen, la Cartera IDUE no queda automàticament inutilitzada, sinó que el seu estat rebaixat a "**operatiu**". Això pot afectar la validesa d' un testimoni TE(C) A/(Q) EAA o d' un certificat qualificat per a signatura o segells electrònics.

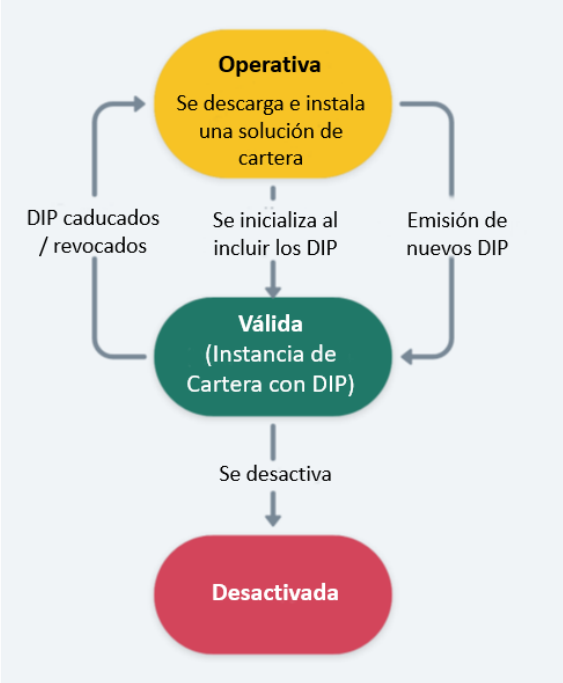


Figura 5: Diagrama d' estat de la instància de cartera

Actualment s'assumeix que només l'Usuari[15] podrà desactivar una Instància de Cartera IDUE. Cal tenir en compte que això és independent de la possibilitat que un prestador de dades DIP/PID o un proveïdor de testimoni TE(C)A/(Q)EAA revoquin els seus testimonis.

[15] Per exemple, en cas de mort de l'usuari o de vulnerabilitat de la seguretat de Cartera IDUE.

5. Requisits per a l'expedició de DIP/PID i TE(C)A/(Q)EAA

5.1. Dades d'identificació de la persona

En aquest capítol es detalla el conjunt DIP/PID presentat per la Cartera IDUE.

Un proveïdor de DIP/PID pot emetre un conjunt de dades DIP/PID per a la cartera IDUE i permetre l'ús de la cartera IDUE com a mitjà d'identificació electrònica en accedir a serveis en línia i fora de línia.

Els mecanismes a través dels quals es genera el DIP/PID i es proporciona a la Cartera IDUE depenen dels Estats membres i només estan limitats per requisits legals com els requisits de nivell d'assegurament (LoA High), RGPD/GDPR o qualsevol altra llei nacional o de la Unió Europea.

A continuació es descriurà el format de les dades tal com es presenten a la Part usuària, sense fer cap suposició sobre com la cartera IDUE va recuperar o generar aquestes dades per endavant.

5.1.1 El conjunt de dades

5.1.2.1. Principis per a la revisió del conjunt DIP/PID

Aquest capítol proposa una revisió dels conjunts de dades opcionals eIDAS especificats en la norma derivada d'eIDAS "CIR 2015/1501"[16] i s'analitzen altres especificacions, la minimització de dades i els identificadors.

La revisió del conjunt de dades opcionals eIDAS que aquí es proposa es construeix sobre la base dels principis següents:

- No hi ha d'haver dues persones amb el mateix conjunt d'atributs obligatoris DIP/PID.
- El conjunt de DIP/PID ha de contenir almenys el conjunt mínim d'atributs especificats en el Reglament d'Execució "CIR 2015/1501" com a obligatoris.

[16] Reglament d'Execució (UE) 2015/1501 de la Comissió, de 8 de setembre de 2015, relatiu al marc d'interoperabilitat de conformitat amb l'article 12, apartat 8, del Reglament (UE) nº 910/2014 del Parlament Europeu i del Consell, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior.

- El conjunt de dades obligatòries es limita per naturalesa a la intersecció (estreta) del que tots els Estats membres poden proporcionar per a totes les persones físiques i jurídiques i el que es necessita a efectes d'identificació electrònica.

5.1.1.1. Atributs del DIP/PID per a persones físiques

La següent taula ofereix una visió general dels atributs DIP/PID inclosos actualment en el marc eIDAS, així com dels atributs opcionals addicionals que se suggereix incloure.

Atributs eIDAS obligatoris	Atributs eIDAS opcionals	Possibles atributs opcionals addicionals
Cognom(s) actual	**Cognom(s) de naixement**	**Nacionalitat/Ciutadania***
Noms actuals	**Noms de naixement**	
Data de naixement	**Lloc de naixement**	**Atributs opcionals utilitzats a nivell nacional, per exemple, número d' identificació fiscal, número de la seguretat social, etc.**
Identificador únic	**Direcció actual**	
	Gènere	

Quadre 2 - Atributs obligatoris i opcionals dels DIP/PID per a les persones físiques

**Nacionalitat/Ciutadania - es tracta d'un possible atribut multivalor perquè els ciutadans poden tenir més d'una nacionalitat. No obstant això, la nacionalitat/ciutadania també pot comunicar-se en forma de TE(C)A/(Q)EAA, per permetre als ciutadans demostrar una nacionalitat determinada, sense actualitzar el conjunt de DIP/PID ni implicar el proveïdor de DIP/PID.*

S' han afegit possibles atributs opcionals addicionals per facilitar una gamma més àmplia d' opcions d' autenticació tant en línia com fora de línia, així com per abordar l' aprenentatge derivat de les actuals implementacions d' eIDAS.

Les metadades associades als DIP/PID poden detallar addicionalment la data d'emissió i/o caducitat, l'autoritat emissora i/o l'Estat membre, la informació necessària per realitzar la vinculació del titular i/o la prova de possessió, la informació o localització dels serveis que es poden utilitzar per consultar l'estat de validesa dels atributs i potencialment més informació.

5.1.2 Requisits d' expedició de l' EPI

En el quadre següent es defineixen els requisits aplicables als DIP/PID en relació amb la informació que s'inclou en el certificat, per exemple, a efectes de comprovació de validesa, autenticitat, validació, polítiques, model de dades i formats.

Les futures versions d' aquest text podran ampliar la taula per especificar requisits. Cal tenir en compte que aquests requisits estan dirigits principalment a la primera versió de les especificacions de la solució Cartera IDUE, i que poden canviar a mesura que evolucionin les especificacions.

#	Logotip
1	**El testimoni sobre DIP/PID HA DE contenir la informació necessària per identificar el proveïdor de DIP/PID.**
2	**El testimoni sobre DIP/PID HA DE contenir la informació necessària per realitzar una comprovació de la integritat de les dades.**
3	**El testimoni sobre DIP/PID HA DE contenir la informació necessària per verificar la seva autenticitat.**
4	**El testimoni sobre DIP/PID HA DE contenir tota la informació necessària per realitzar comprovacions de l'estat de validesa del testimoni.**
5	**El testimoni sobre DIP/PID HA d'incloure tota la informació (com a atribut o com qualsevol altre valor signat) necessària per realitzar la verificació de la vinculació del titular per una Part Informada.**
6	**El testimoni sobre DIP/PID S'ha d'emetre per ser presentada d'acord tant amb el model de dades especificat en la norma ISO/IEC 18013-5:2021 com amb el Model de dades de credencials verificables v1.1 del W3C.**
7	**El testimoni sobre DIP/PID S'ha de codificar com a CBOR i en format JSON.**
8	**El testimoni sobre DIP/PID HA de permetre la divulgació selectiva d'atributs mitjançant l'ús de l'esquema "Selective Disclosure for JWTs (SD-JWT)" i "Mobile Security Object (ISO/IEC 18013-5)" d'acord amb el model de dades (Permís de conduir al mòbil).**
9	**El testimoni sobre DIP/PID HA d'utilitzar firmes electròniques i formats de xifrat tal com es detalla a la RFC 8812 Concise Binary Object Representation (CBOR) Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms.**
10	**El testimoni sobre DIP/PID HA d'utilitzar algoritmes de signatura i xifrat de conformitat amb la norma SOG-IS ACM (Agreed Cryptographic Mechanism)[17].**

Quadre 3 - Requisits d'expedició d'EPI

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

5.2. Testimoni electrònic d'atribut qualificat i no qualificat

5.2.1 Requisits d' expedició dels TE(C) A/(Q) EAA

En el quadre següent es defineixen els requisits aplicables als Testimonis TE(C) A/(Q) EAA en relació amb la informació que s' inclou en el Testimoni, per exemple, a efectes de comprovació de validesa, autenticitat, validació, polítiques relacionades amb la gestió de claus, el model de dades i els formats.

Els testimonis TE(C)A/(Q)EAA també es poden emetre d'acord amb els requisits aplicables a les Dades DIP/PID.

Les futures versions d' aquest text podran ampliar la taula per especificar requisits. Cal tenir en compte que aquests requisits estan dirigits principalment a la primera versió de les especificacions de la solució Cartera IDUE, i que poden canviar a mesura que evolucionin les especificacions.

#	Logotip
1	**Els testimonis TE(C) A/(Q) EAA HAN de contenir la informació necessària per identificar l' Emissor.**
2	**Els testimonis TE(C)A/(Q) EAA HA DE Ncontenir la informació necessària per realitzar una comprovació de la integritat de les dades.**
3	**Els testimonis TE(C)A/(Q) EAA HAN de contenir la informació necessària per verificar la seva autenticitat.**
4	**Els testimonis TE(C) A/(Q) EAA HAN de contenir tota la informació necessària per realitzar comprovacions del seu estat de validesa.**
5	**(no s'indica)**
6	**Els testimonis TE(C)A/(Q)EAA HAURIEN d'incloure tota la informació (com a atribut o com qualsevol altre valor signat) necessària per realitzar la verificació de la vinculació del titular per part d'una Part Informada.**
7	**Els testimonis TE(C)A/(Q)EAA S'han d'expedir de conformitat amb una de les especificacions del model de dades: la norma de codificació de permís de conduir: I"SO/IEC 18013-5:2021", o "Verifiable Credentials Data Model v1.1" (Model de dades de credencials verificables 1.1) del W3C.**
8	**Els testimonis TE(C)A/(Q)EAA haurien de codificar-se com un dels següents formats: CBOR o JSON segons el model de dades utilitzat per a la certificació. Veure RFC 8812, RFC 8152, RFC 9052, RFC 9053**

9	**Els testimonis TE(C)A/(Q)EAA PODEN codificar-se com a JSON-LD (JSON for Linking Data).**
10	**Els testimonis TE(C)A/(Q)EAA HAURIEN de permetre la Revelació Selectiva d'atributs utilitzant bé "Selective Disclosure for JWTs" (Revelació Selectiva per a JWTs) (SD-JWT) o bé l'esquema "Mobile Security Object" (Objecte de Seguretat Mòbil) de la norma sobre permís de conduir (ISO/IEC 18013-5) d'acord amb el model de dades utilitzat per al testimoni.**
11	**Els testimonis TE(C)A/(Q)EAA HAURIEN d'utilitzar un dels següents formats de signatura i xifrat segons es detalla en les normes de l'IETF, RFC relatives a JOSE (Javascript Object Signing and Encryptio), i RFCs relatives a COSE (CBOR Object Signing and Encryption) RFCs d'acord amb el model de dades utilitzat per al testimoni.**
12	**Els testimonis TE(C)A/(Q)EAA HAURIEN d'utilitzar algoritmes de xifrat de conformitat amb la norma SOG-IS ACM (Agreed Cryptographic Mechanism)**
13	**Els testimonis TE(C)A/(Q)EAA HAURIEN d'emetre's d'acord amb el protocol OpenID4VCI (OpenID for Verifiable Credential Issuance).**

Quadre 4 - Requisits d'expedició de les (Q)CEA

6. Arquitectura de referència i fluxos

L' arquitectura de referència representa un conjunt de decisions preses durant el procés de disseny de l' arquitectura de les solucions de Cartera IDUE. Aquestes eleccions es van basar en la necessitat que les solucions de Cartera IDUE suportin diversos escenaris en els quals l'usuari, la part que confia (o part informada), o tots dos, estiguin fora de línia, alhora que proporcionen flexibilitat als Estats membres per implementar una solució de Cartera IDUE en diverses configuracions de components.

6.1. Consideracions sobre el disseny

Per limitar la complexitat, les especificacions inicials de la Solució de Cartera IDUE inclouran només un nombre mínim de components de la solució que permetin l'ús de la Instància de Cartera IDUE per a la identificació de l'Usuari, de manera que pugui funcionar com un mitjà d'Identitat Electrònica (eID).

Les opcions triades no reflecteixen una importància relativa ni un compromís a llarg termini. En el seu lloc, la selecció s'ha guiat per factors com la disponibilitat i maduresa de les normes i especificacions, una estimació de la facilitat d'adopció i el grau de flexibilitat (en termes de casos d'ús permesos) que ofereix cada component de la solució.

Els components de la solució aquí proposats evidencien l'expectativa actual d'utilitzar la sèrie de normes ISO/IEC 23220, una vegada disponibles públicament, per a futures versions de l'ARF (Cards and security devices for personal identification — Building blocks for identity management via mobile devices).

6.2. Components d'arquitectura

Els següents components han estat identificats com els blocs de construcció de l' arquitectura de la cartera IDUE necessaris per implementar una Solució de Cartera IDUE:

- **Sistema de gestió de claus criptogràfiques.** Aquest component s'encarrega de gestionar i emmagatzemar informació criptogràfica com les claus privades generades, per exemple, durant el procés d'emissió de DIP/PID.

- **Protocol d' intercanvi de testimonis**. Aquest protocol defineix com sol·licitar i presentar les dades DIP/PID i els testimonis TE(C)A/(Q)EAA de forma segura i preservant la privacitat. El protocol també defineix com es realitza l'autenticació entre la Part que Confia (o Part Informada) i la Instància de Cartera IDUE, en particular el mecanisme a través del qual la Part Informada pot sol·licitar la identificació a través de la Cartera IDUE. La sol·licitud conté tota la informació necessària sobre la Part Informada i les dades sol·licitades. Aquest protocol s' ocupa de la negociació de la confiança i l' autenticació mútua.

- **Protocol d' emissió**. El protocol defineix com s'han d'expedir els DIP/PID i els testimonis TE(C)A/(Q)EAA i en quins formats.

- **Model de dades**. El model de dades defineix i descriu els elements de dades i com interactuen entre si i les seves propietats.

- **Esquemes DIP/PID i TE(C)A/(Q)EAA**. L' esquema de testimoni conté l' estructura i l' organització lògica de les dades que defineixen les propietats del testimoni, els atributs de l' Usuari. L'esquema de testimoni també conté informació addicional que inclou, entre altres coses, els mecanismes de verificació, la garantia d'identitat subjacent (nivell d'assegurament) i el marc de confiança amb què es relacionen les propietats, així com la prova de possessió per part de l'usuari legítim.

- **Formats de DIP/PID i TE(C)A/(Q)EAA**. Els formats de DIP/PID i TE(C)A/(Q)EAA s'utilitzen per representar la característica, qualitat, dret o permís d'una persona física o jurídica o d'un objecte, en forma d'artefactes digitals signats electrònicament i verificables, que contenen qualsevol propietat addicional a efectes d'interoperabilitat.

- **Formats de signatura**. Implementació tècnica d'un o diversos mètodes matemàtics en forma d'artefacte digital, destinada a demostrar l'autenticitat d'un document digital, la seva integritat, autenticar l'autor d'un document i, opcionalment, també el seu destinatari (audiència del document).

- **Model de confiança.** Conjunt de normes que garanteixen la legitimitat dels components i les entitats que intervenen en la infraestructura de Cartera IDUE, i que abasten:
  - Autenticació d' usuaris.
  - Identificació de l' emissor.
  - Registre d' emissors.
  - Models de dades i esquemes reconeguts.
  - Registre i autenticació de les parts Informades.
  - Mecanismes per establir la confiança en un escenari multidomini.

  Els components del model de confiança permeten identificar les entitats que confien en Cartera IDUE i són fonamentals per a l'autenticitat, confidencialitat, integritat i el consentiment informat (en les signatures electròniques i segells) de la informació. Existeixen diferents models de confiança basats en diferents normes.
  La llista de confiança és un mecanisme en el marc d'un model de confiança per publicar i obtenir informació sobre parts que ostenten autoritat, per exemple, emissors de DIP/PID, de testimonis TE(C)A/(Q)EAA i parts informades.

- **Suites i mecanismes criptogràfics**. Algoritmes i mètodes que asseguren l' intercanvi de dades en termes de confidencialitat i integritat.

- **Identificadors d' entitat**. Identificadors únics per a tots els elements del model de dades.

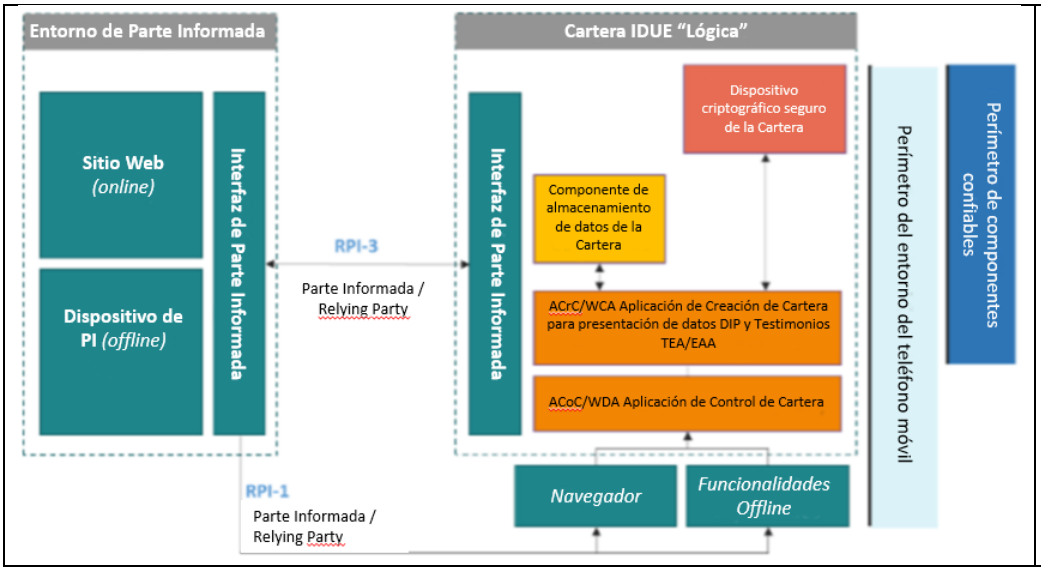
- **Comprovació de l' estat de validesa**. Mecanisme per publicar i obtenir informació sobre l'estat de validesa de, entre d'altres, de dades DIP/PID, de testimonis TE(C)A/(Q)EAA, certificats destinats a realitzar signatures o segells electrònics, etc.

6.3. Arquitectura lògica

Quan una solució de Cartera IDUE té una aplicació que s'executa en un dispositiu mòbil, pot existir la necessitat de components de confiança addicionals que no formen part d'aquesta aplicació però que, no obstant això, formen part dels recursos lògics de la Cartera IDUE. Aquesta necessitat pot sorgir per diverses raons:

- Seguretat: per exemple, si un dispositiu concret no disposa de maquinari prou segur, com un "Secure Element" (element segur, equipament estàndard de molts mòbils), poden ser necessaris components de maquinari externs, com targetes intel·ligents.
- Reutilització de sistemes en entorns de servidor remot (backend).
- Reutilització de la infraestructura d'identitat centrada en l'usuari (denominada de vegades identitat descentralitzada).

Aquests components de confiança poden ser: emmagatzematge extern de confiança, maquinari extern o integrat de confiança o altres components remots de Cartera IDUEs. A continuació, es mostra una representació conceptual de les variacions en la implementació dels components de Cartera IDUE:



ACrA/WCA: Crea la presentació (verificable) de DIP i Testimonis Qualificats que es comparteixen amb la Part informada, segons la informació rebuda de l'ACoC/WDA.
ACoC/WDA: Proporciona les dades triats per l'usuari:

- DIP i testimonis (que es poden combinar)

	• Determina quines es poden (o no) presentar

Figura 6: Model conceptual de les configuracions de Cartera IDUE

La taula següent relaciona els components de la cartera IDUE amb el model conceptual de la figura 6.

Bloc funcional en el model conceptual	Components aplicables a la solució de Cartera IDUE
Dispositiu criptogràfic segur de la Cartera IDUE	Claus d' usuari i certificats
	Entorn segur i aïllat per a claus i dades
	Algoritmes criptogràfics (per exemple, simètrics, asimètrics, derivació de claus, funcions hash, generació de números aleatoris) i protocols (per exemple, ECDH, TLS).
	Entorn segur definit per hardwqre per a claus i dades: un Element Segur (SE), Entorns d'Execució de Confiança (Trusted Execution Environment -TEEs), Mòdul de Seguretat de Hardware (Hardware Security Module - HSM), etc. (remot o local).
	Dades d'autenticació (PIN, biometria)
Components d' emmagatzematge de dades de la cartera IDUE	Identificador únic i persistent de l' usuari
	Atributs de l' usuari
	Dades personals i atributs de l' usuari
	Entorn segur per a claus i dades
Cartera IDUE "Presentació de DIP/PID o TEA/EAA" Aplicació de creació de Cartera (WCA - Wallet Creation Application)	Registres, historial d' operacions de la Instància de Cartera IDUE, telemetria
	Identificador de la Instància d'aplicació Cartera IDUE (per exemple, configuració, fabricant i versió)
	Interfícies internes de la instància de Cartera IDUE (per exemple, entre emmagatzematge, components, xifrat)
Aplicació de control de Cartera IDUE (WDA, Wallet Driving Application)	Registres, historial d' operacions de la Instància de Cartera IDUE, telemetria
	Identificador de l'aplicació d'Instància de Cartera IDUE (per exemple, configuració, fabricant i versió)

	Interfície d' usuari de la Cartera IDUE
Interfície de la part informada	Interfície de la Cartera IDUE amb (Q)TSP, amb proveïdors de TE(C)A/(Q)EAA, infraestructures dels Estats membres, e-ID nacionals, parts que confien i altres fonts d'EEA.
	Canals de comunicació (en línia/fora de línia) entre la cartera IDUE i altres parts

Taula 5 - Correspondència entre els components de la cartera IDUE i els blocs funcionals del model conceptual

La taula següent assigna els components de la Cartera IDUE als dos perímetres representats a la Figura 6.

Perímetres	**Components aplicables a la solució Cartera IDUE**
Perímetres dels possibles components de confiança	Informació sobre el dispositiu (tipus, configuració, versió de firmware, estat, etc.)
	Claus i certificats del sistema
	Sistemes back-end (servidors de bases de dades)
	Dispositius connectats de confiança
Perímetre mòbil potencial	Informació sobre el dispositiu (tipus, configuració, versió de firmware, estat, etc.)
	Sensors de l' smartphone: càmera, lector NFC, sensor d' empremtes dactilars, acceleròmetre, etc.

Quadre 6: correspondència entre els components de la cartera IDUE i els perímetres

6.4. Tipus de fluxos

Aquesta secció descriu els quatre tipus de fluxos que Cartera IDUE HA DE suportar a nivell general. Els quatre fluxos són els següents:

1. Flux supervisat de proximitat.
2. Flux de proximitat no supervisat.
3. Flux remot entre dispositius.
4. Flux remot del mateix dispositiu.

Els fluxos 1 i 2 estan relacionats amb un escenari en el qual l'usuari de Cartera IDUE es troba físicament a prop d'una part que confia (part informada) i l'intercanvi i la divulgació de

testimonis (DIP/PID i/o TECA/QEAA) s'han de produir utilitzant protocols de proximitat (NFC, Bluetooth, QR-Code, etc.), sense que l'usuari tingui connectivitat a Internet (nòtese que això no implica que sigui possible qualsevol altra funció a part del transport sense connexió). Els dos fluxos de proximitat difereixen en un aspecte important. En el flux supervisat, la Cartera IDUE presenta atributs verificables a, o sota la supervisió de, una persona que actua com a part informada (que pot operar un dispositiu propi). En el flux no supervisat, la Cartera IDUE presenta atributs verificables a una màquina sense supervisió humana.

Els fluxos 3 i 4 estan relacionats amb un escenari en el qual l' intercanvi de dades s' ha de produir a través d' Internet. Els dos fluxos remots difereixen en un aspecte important. En el flux remot entre dispositius, l'usuari de la Cartera IDUE consumeix informació del servei en un dispositiu diferent del dispositiu de la Cartera IDUE, que només s'utilitza per assegurar la sessió (per exemple, utilitzant Cartera IDUE per escanejar un codi QR en una pàgina d'inici de sessió per accedir a un compte bancari al seu navegador web). En canvi, en el flux remot del mateix dispositiu, l'usuari de Cartera IDUE utilitza el dispositiu de la Cartera IDUE tant per assegurar la sessió com per consumir la informació del servei.

Les experiències dels usuaris es basaran en almenys un dels quatre fluxos descrits, i probablement en una combinació d' ells. Observeu que els quatre fluxos poden implementar-se de múltiples maneres. Les implementacions específiques queden fora de l' àmbit d' aquest text.

Cal seguir estudiant els dos fluxos de proximitat, ja que són possibles amb o sense connexió a Internet. Entre els possibles escenaris figuren:

- l'Usuari i la Part Informada estan tots dos en línia,
- només l'Usuari està connectat,
- només la Part Informada està en línia,
- L'usuari i la Part Informada estan desconnectats.

Per a tots els fluxos descrits anteriorment i, en concret, per al flux no supervisat de proximitat, l' autorització de l' usuari és un requisit previ per a l' intercanvi de dades.

A continuació, es detallen les configuracions inicials del DIP/PID i del TEA/EAA (en el futur podran afegir-se configuracions segons sigui necessari).

6.5. Configuracions de la cartera

6.5.1. Justificació

Un dels objectius del desenvolupament de la Cartera IDUE és harmonitzar les dades DIP/PID i els testimonis TE(C)A/(Q)EAA a través de les fronteres. Idealment, això implica un nombre molt reduït de solucions tècniques diferents per limitar la complexitat, la qual cosa facilita la implantació i adopció. D' altra banda, l' especificació de Cartera IDUE ha de donar suport a una àmplia gamma de casos d' ús amb diferents requisits. Aquestes diferències motiven formes específiques de crear, sol·licitar i presentar dades DIP/PID i testimonis TE(C)A/(Q)EAA. Per satisfer aquestes necessitats, les solucions de Cartera IDUE implementaran configuracions. Una configuració és un conjunt específic de restriccions i formes d'utilitzar les capacitats tècniques de la Solució de Cartera IDUE per gestionar tant el conjunt de DIP/PID com els testimonis TE(C)A/(Q)EAA.

El primer propòsit d' una configuració és vincular les capacitats específiques de la Cartera IDUE amb els requisits dels casos d' ús que es poden complir amb aquestes capacitats. Una sola configuració ha de suportar múltiples casos d' ús; cadascun conforme a la configuració específica per a la qual es va emetre el DIP/PID o el testimoni TE(C)A/(Q)EAA.

El segon i últim propòsit d' una configuració és proporcionar una eina per ampliar potencialment els entorns tecnològics i les característiques de les especificacions de la Solució de Cartera IDUE. Si un cas d' ús, o un grup de casos d' ús, no es pot basar en una configuració existent de la Solució de Cartera IDUE, s' introdueix la necessitat d' incloure una configuració addicional per donar suport als requisits que no es poden satisfer amb les configuracions existents. En el capítol 8 es descriuen la governança i el procés per afegir noves configuracions.

6.5.2. Configuracions inicials

Les Solucions de Cartera IDUE admetran inicialment dues configuracions:

- La configuració de **tipus 1** està dirigida específicament als casos d'ús en els quals la part Informada confia en les garanties requerides per al nivell d'assegurament alt de la identitat (LoA High), tal com es defineix en el Reglament d'Execució CIR 2015/1502[18] per permetre la identificació transfronterera utilitzant atributs DIP/PID en nivell d'assegurament de la identitat (LoA High). La configuració de Tipus 1 està dissenyada principalment per a fins d'establiment de dades d'identitat DIP/PID.
- La configuració de **Tipus 2** té com a objectiu permetre flexibilitat i suport de característiques addicionals per a possibles casos d'ús de testimonis TE(C)A/(Q)EAA

[18] Reglament d'Execució (UE) 2015/1502 de la Comissió, de 8 de setembre de 2015, pel qual s'estableixen especificacions tècniques mínimes i procediments relatius als nivells de garantia dels mitjans d'identificació electrònica de conformitat amb l'article 8, apartat 3, del Reglament (UE) nº 910/2014 del Parlament Europeu i del Consell, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior.

que no puguin ser satisfets per la configuració de Tipus 1 (per exemple, possiblement en àrees de salut, credencials d'educació, ...).

Cal tenir en compte que la configuració de Tipus 1 no està pensada únicament per al conjunt de DIP/PID. És probable que molts testimonis TE(C)A/(Q)EAA s'utilitzin en àmbits que requereixin nivells d'assegurament alts (per exemple, finances, sanitat, accés a edificis) i tinguin requisits que se satisfacin amb la configuració de Tipus 1. Si és així, aquests TE(C) A/(Q) EAA s' expediran d' acord amb la configuració de Tipus 1.

6.5.3. Requisits de configuració

Aquesta secció estableix els requisits de les configuracions comparant la configuració de Tipus 1 i Tipus 2 en diferents grups de requisits. Les futures versions d' aquest text podran ampliar la taula per especificar els requisits relatius, per exemple, als Emissors i a les Parts que Confien. Cal tenir en compte que aquests requisits estan dirigits principalment a la primera versió de les especificacions de la Solució de Cartera IDUE, i que poden canviar a mesura que evolucionin les especificacions.

La següent taula defineix els requisits aplicables als components de la Solució de Cartera IDUE per suportar les dues configuracions. Segons el tipus de configuració el requisit implica substituir els punts suspensius [...] pel verb indicat a la columna Tipus 1 o Tipus 2 (DEBE, HAURIA, etc).

Component	**Logotip**	**Tipus 1**	**Tipus 2**
Sistema de gestió de claus criptogràfiques - 1	La Solució de Cartera IDUE [...] basar-se en un dels següents components per emmagatzemar i gestionar claus criptogràfiques: Element segur (SE) integrat o entorn de (per a dispositius mòbils), dependència d'un dispositiu extern (elements segurs / targetes intel·ligents), i un servidor (mòdul de seguretat de maquinari remot). L' elecció del maquinari segur que s' utilitzarà i suportarà depèn de cada solució de Cartera IDUE.	HA DE	HAURIA
Sistema de gestió de claus criptogràfiques - 2	La Solució de Cartera IDUE [...] aplicar mesures de seguretat per evitar l'exportació de secrets criptogràfics.	HA DE	HAURIA

Protocol d'intercanvi de testimonis - 1	La Solució de Cartera IDUE [...] suportar OpenID4VP com a protocol d'intercanvi de testimonis per **a fluxos remots.** Quan es demana autenticació pseudònima, els paràmetres de sol·licitud S'HAURIEN d'especificar d'acord amb l'especificació OpenID SIOPv2.	HA DE	POT
Protocol d'intercanvi de testimonis - 2	La Solució de Cartera IDUE [...] suportar el protocol detallat en la norma ISO/IEC 18013-5:2021 per **a fluxos de proximitat**.	HA DE	POT
Protocol d'intercanvi de testimonis - 3	La Solució de Cartera IDUE [...] realitzar comprovacions per fer complir la vinculació de sessió (és a dir, sol·licitud d'atribut per a DIP/PID).	HAURIA	POT
Protocol d'intercanvi de testimonis - 4	La Solució de Cartera IDUE [...] suportar alternatives de protocol d'intercanvi de testimonis[19].	POT	POT
Protocol d'intercanvi de testimonis - 5	La Solució de Cartera IDUE [...] poder realitzar una prova de possessió.	HA DE	POT
Protocol d'intercanvi de testimonis - 6	La Solució de Cartera IDUE [...] suportar la Divulgació Selectiva d'atributs tal com s'especifica en la norma ISO/IEC 18013-5:2021.	HA DE	POT
Protocol d'intercanvi de testimonis - 7	La Solució de Cartera IDUE [...] suportar la Divulgació Selectiva d'atributs com s'especifica en l'especificació SD-JWT.	HA DE	POT
Protocol d'emissió - 1**	La Solució de Cartera IDUE [...] admetre OpenID4VCI com a protocol d'emissió. Els Estats membres són lliures d' incloure alternatives addicionals al protocol d' emissió en les seves solucions nacionals.	HA **	HA DE

[19] Cal destacar l'API REST de mdoc, tal com es detalla en l'esborrany e lanorma ISO/IEC 23220-4.

Model de dades -1	La Solució de Cartera IDUE [...] admetre testimonis emesos de conformitat amb el model de dades especificat en la norma ISO/IEC 18013-5:2021.	HA DE	HAURIA
Model de dades -2	La Solució de Cartera IDUE [...] suportar testimonis emesos d'acord amb el model de dades especificat en l'especificació W3C Verifiable Credentials Data Model 1.1.	HA DE	HAURIA
Formats DIP/PID i TE(C)A/(Q)EAA - 1	La Solució de Cartera IDUE [...] suportar testimonis en format JWT i SD-JWT.	HA DE	POT
Formats DIP/PID i TE(C)A/(Q)EAA - 2	La Solució de Cartera IDUE [...] admetre testimonis en format CBOR.	HA DE	POT
Formats DIP/PID i TE(C)A/(Q)EAA - 3	La Solució de Cartera IDUE [...] suportar testimonis en format JSON-LD.	POT	POT
Formats de signatura -1	La Solució de Cartera IDUE [...] suportar formats de signatura electrònica i xifrat d'acord amb les especificacions JOSE (JWT).	HA DE	POT
Formats de signatura - 2	La Solució de Cartera IDUE [...] suportar formats de signatura i xifrat d'acord amb les especificacions COSE.	HA DE	POT
Formats de signatura - 3	La Solució de Cartera IDUE [...] admetre formats de signatura i xifrat d'acord amb les especificacions LD-Proof.	NO HA DE	POT
Suites i mecanismes criptogràfics - 1	La Solució de Cartera IDUE [...] suportar suites criptogràfiques i mecanismes utilitzats per a atributs detallats en SOG-IS Agreed Cryptographic Mechanisms Version 1.2.	HA DE	HAURIA

Taula 7 - Requisits de configuració

***Només per a testimonis TE(C)A/(Q)EAA que han de tenir un protocol d'emissió comú per garantir la interoperabilitat. En el cas de les dades DIP/PID, correspon a l'Estat membre*

definir el protocol d'emissió i cada solució de cartera suportarà el protocol d'emissió de DIP/PID específic d'acord amb les especificacions de l'Estat membre.

Les solucions de Cartera IDUE **HAN** de suportar la configuració de **Tipus 1** que és obligatòria per al DIP/PID.

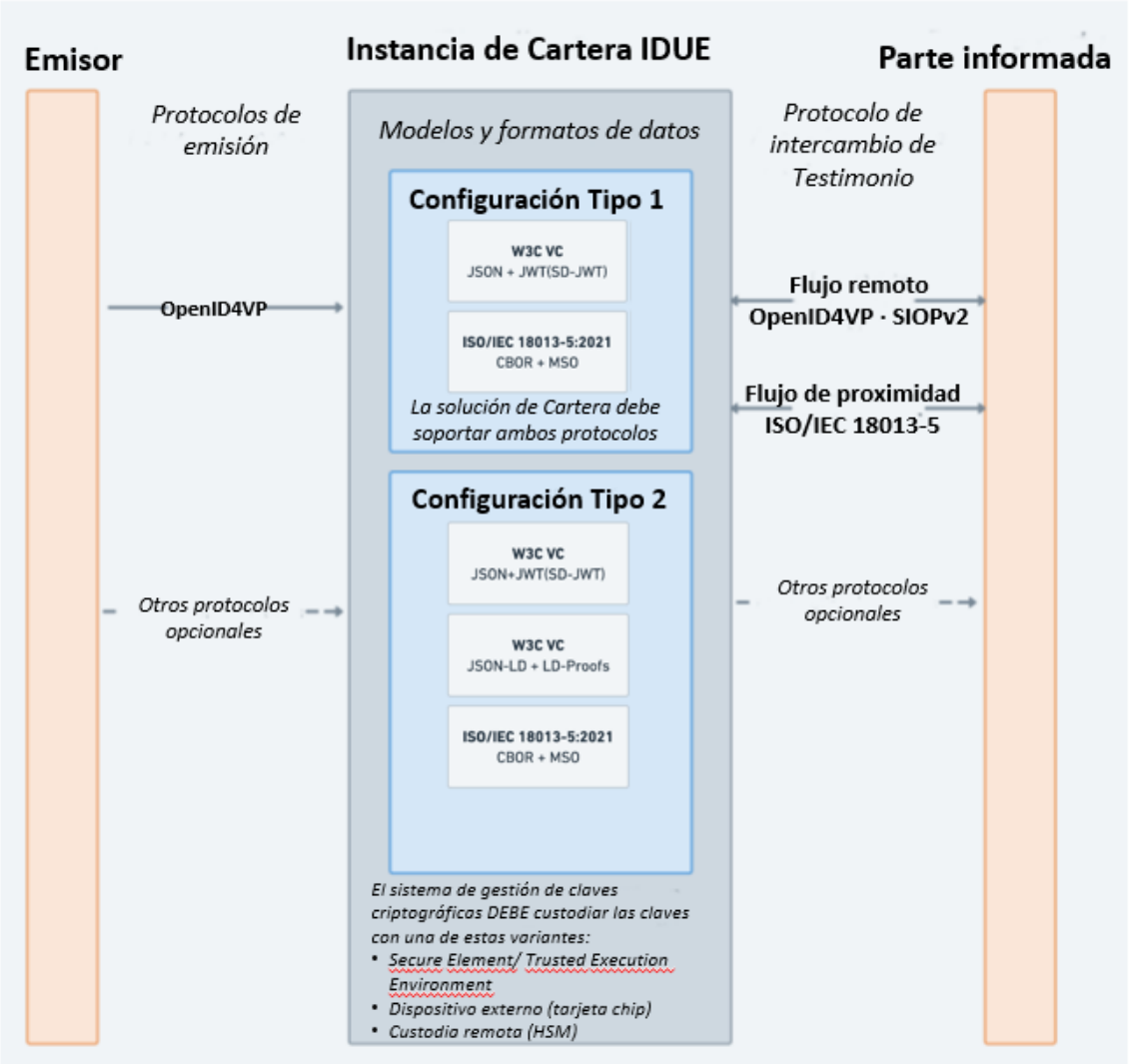


Figura 7. Configuracions Cartera IDUE.

7. El procés de certificació de les carteres IDUE

Els Estats membres, de conformitat amb l'article 6 de la proposta de reforma del Reglament EIDAS, han de designar els organismes d'avaluació de la conformitat acreditats que supervisaran la realització de l'avaluació de la conformitat de les carteres IDUE. Aquest procés de designació s' ha d' harmonitzar entre els Estats membres.

Una vegada efectuada aquesta designació, els Estats membres comunicaran a la Comissió Europea els noms i adreces d' aquests organismes públics o privats d' acord amb l' apartat 5 de l' article 6 quater de l' esmentada proposta.
El proveïdor de la cartera IDUE ha de sol·licitar (seleccionar, contractar) un o diversos OEC/CAB designats que avaluïn i certifiquin la conformitat de la seva cartera IDUE amb els requisits del Reglament eIDAS.

La certificació de la Cartera IDUE la duu a terme l'OEC/CAB per avaluar i certificar la conformitat de la Cartera IDUE (objectiu de la certificació) amb els documents normatius que es derivin dels actes d'execució establerts a l'Art.

La Cartera IDUE haurà d' estar certificada per garantir les avaluacions de conformitat, però també per demostrar el compliment d' alts nivells de seguretat. L'ús d'un sistema de certificació de la ciberseguretat hauria d'aportar un nivell harmonitzat de confiança en la seguretat de la Cartera IDUE. S'espera que l'emmagatzematge segur de material criptogràfic també estigui subjecte a la certificació de ciberseguretat.

El procés de certificació dels proveïdors de carteres IDUE ha d' aprofitar, basar-se i exigir l' ús dels sistemes de certificació pertinents i existents del Reglament sobre la Ciberseguretat,[20] o parts dels mateixos, per certificar la conformitat de les carteres, o parts dels mateixos, amb els requisits de ciberseguretat aplicables.

[20] REGLAMENT (UE) 2019/881 DEL PARLAMENT EUROPEU I DEL CONSELL de 17 d'abril de 2019 relatiu a ENISA (Agència de la Unió Europea per a la Ciberseguretat) i a la certificació de la ciberseguretat de les tecnologies de la informació i la comunicació i pel qual es deroga el Reglament (UE) n.o 526/2013 («Reglament sobre la Ciberseguretat»)

8. Procés de desenvolupament de l' Arquitectura i del Marc de referència

8.1. Publicació

Aquest document i els elements pendents es posen a disposició del públic a l' adreça electrònica https://code.europa.eu/eudi/architecture-and-reference-framework, on s' actualitzarà periòdicament segons el flux de treball descrit al capítol 8.2.

8.2. Actualització

Per garantir un progrés constant i ràpid en l' elaboració i actualització d' aquest document, s' aplica el següent procés i metodologia de treball.

El Grup d'Experts eIDAS (E03032)[21] haurà de mantenir un backlog, que és una llista prioritzat d'elements de treball per completar l'ARF. La llista de tasques pendents s'actualitzarà en funció dels comentaris del Grup d'Experts eIDAS, els Projectes Pilot a Gran Escala impulsats des de l'Agència HaDEA (DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID[22]), la Comissió o altres parts interessades, com les organitzacions internacionals de normalització. Per exemple, els resultats del desenvolupament de la implementació de referència de la Cartera IDUE (Framework Contract for Fixed Price and Quoted Time and Means for Development, Consultancy and Support for the European Digital Identity Wallet[23]) i els consegüents esborranys d'especificacions tècniques detallades poden donar lloc a nous elements de treball.

La Comissió Europea (DGN) organitzarà el treball sobre els temes endarrerits i facilitarà que el treball avanci segons el calendari previst.

El Grup d' Experts d' eIDAS debatrà i compararà periòdicament diferents propostes relatives a solucions tècniques, recomanacions i requisits relacionats amb cada qüestió pendent pertinent amb vista a actualitzar l' ARF. Referent a això, el Grup d'Experts eIDAS mantindrà una llista de Registres de Decisions d'Arquitectura (RDA, en anglès ADR, Architecture Decission Records), de manera que sigui possible fer un seguiment i comprendre la motivació que subjau a les decisions tècniques descrites a l'ARF.

Qualsevol canvi i/o actualització d'aquest document haurà de ser acordat pel Grup d'Experts eIDAS. El Grup d' Experts eIDAS es reunirà periòdicament amb l' objectiu de debatre i aprovar

[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

noves versions d' aquest document, així com d' actualitzar els treballs pendents de desenvolupament.

Aquest document s' adaptarà al resultat de les negociacions legislatives de la proposta de Marc Europeu d' Identitat Digital i s' actualitzarà en conseqüència.

8.2.1. Versions de documents

Per evitar problemes d' interoperabilitat i que els canvis en l' ARF passin desapercebuts, s' utilitzarà per a l' ARF un sistema de control de versions i el següent esquema semàntic de versions.

El document ARF tindrà un número de versió determinat seguint el format *MAJOR. MENOR. PARCHE*, on:

La versió **MAJOR** s'incrementa (és a dir, hi ha una nova versió), quan el document ARF ha patit canvis significatius, per exemple, introduint alguns canvis radicals en l'arquitectura,

La versió **MENOR** s' incrementa quan s' ha afegit nova informació al document o se n' ha eliminat informació, i

La versió **PARCHE** s'incrementa quan s'han realitzat canvis menors (per exemple, correcció d'errades).

9. Referències

[Paraules clau en l'ARF per indicar els nivells d'exigència] 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. i D. Chadwick, "Verifiable Credentials Data Model 1.0", 19 de novembre de 2019, <https://www.w3.org/TR/vc-data-model>.

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

[OpenID4VCI] Lodderstedt, T., Yasuda, K., i T. Looker, "OpenID for Verifiable Credential Issuance", 30 de desembre 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 gener 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

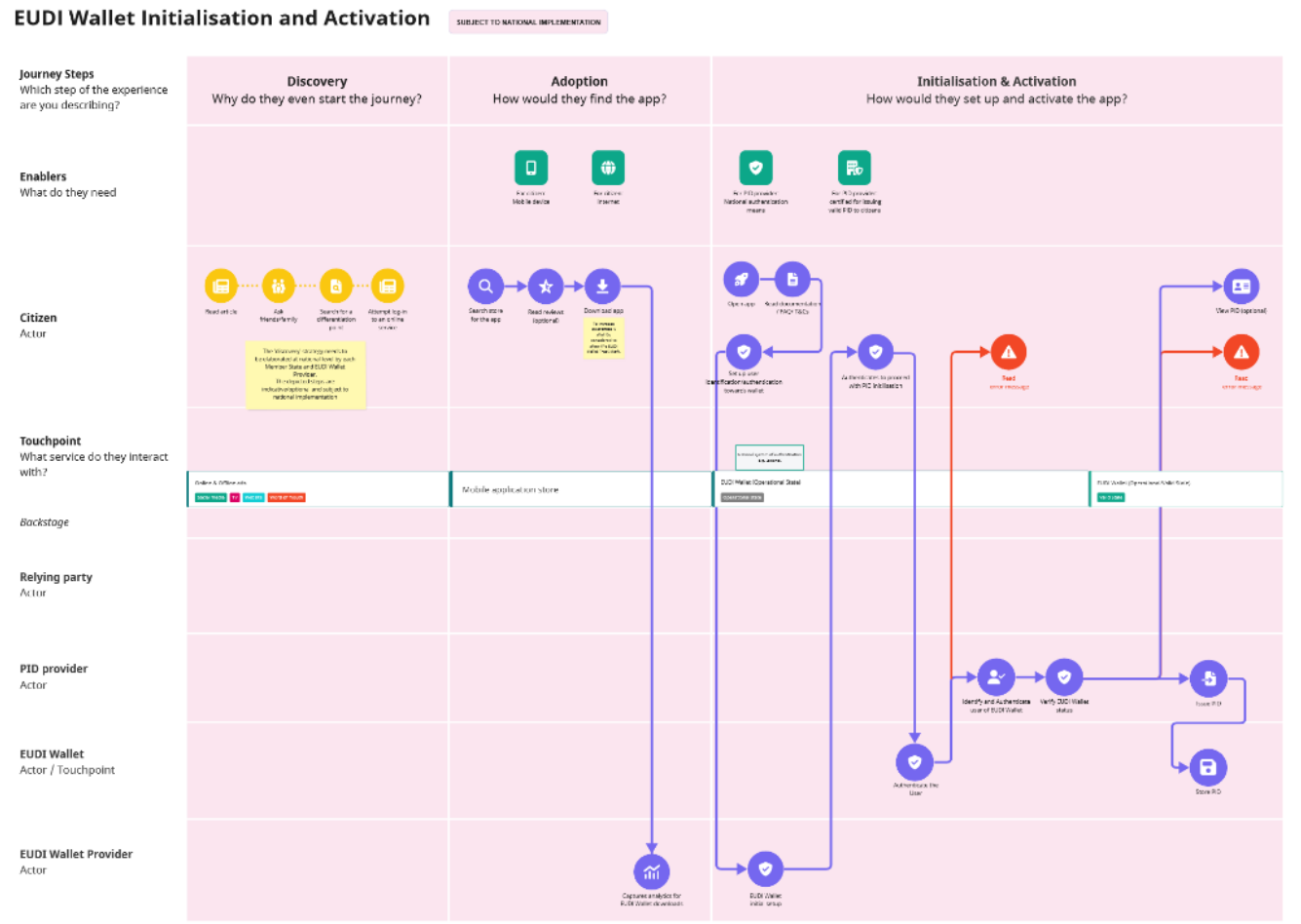
[JOSE] RFC7515 https://www.rfc-editor.org/rfc/rfc7515.html,
RFC7516 https://www.rfc-editor.org/rfc/rfc7516.html,
RFC7517 https://www.rfc-editor.org/rfc/rfc7517.html,
RFC7518 https://www.rfc-editor.org/rfc/rfc7518.html

[SOG-IS] Mecanismes criptogràfics acordats 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/

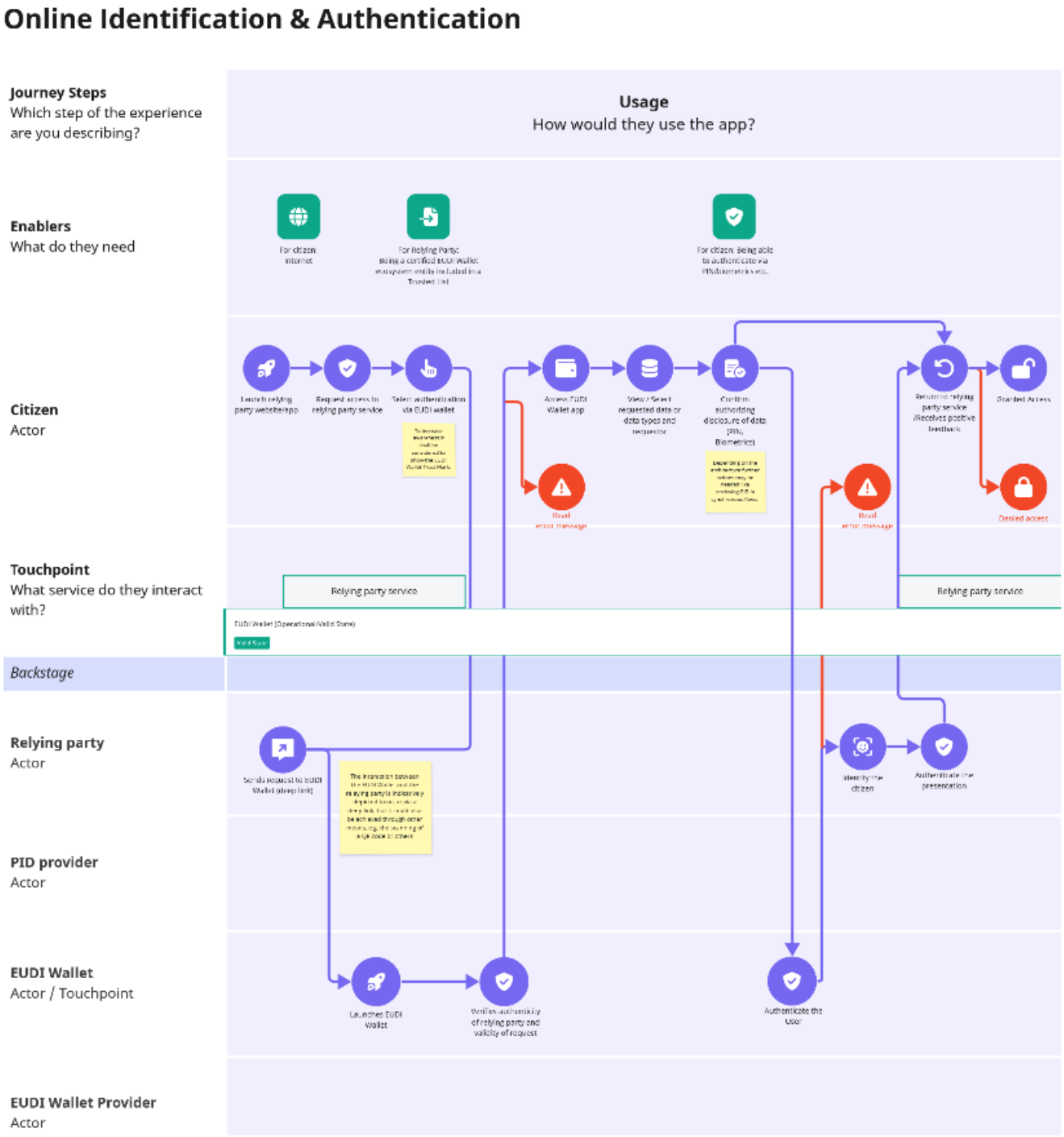
Annex 01 - inicialització i activació

El model de servei sobre la inicialització i activació de la Cartera es descriu a l'arxiu adjunt ***Annex 01- EUDI Wallet - Initialisation and Activation.pdf***



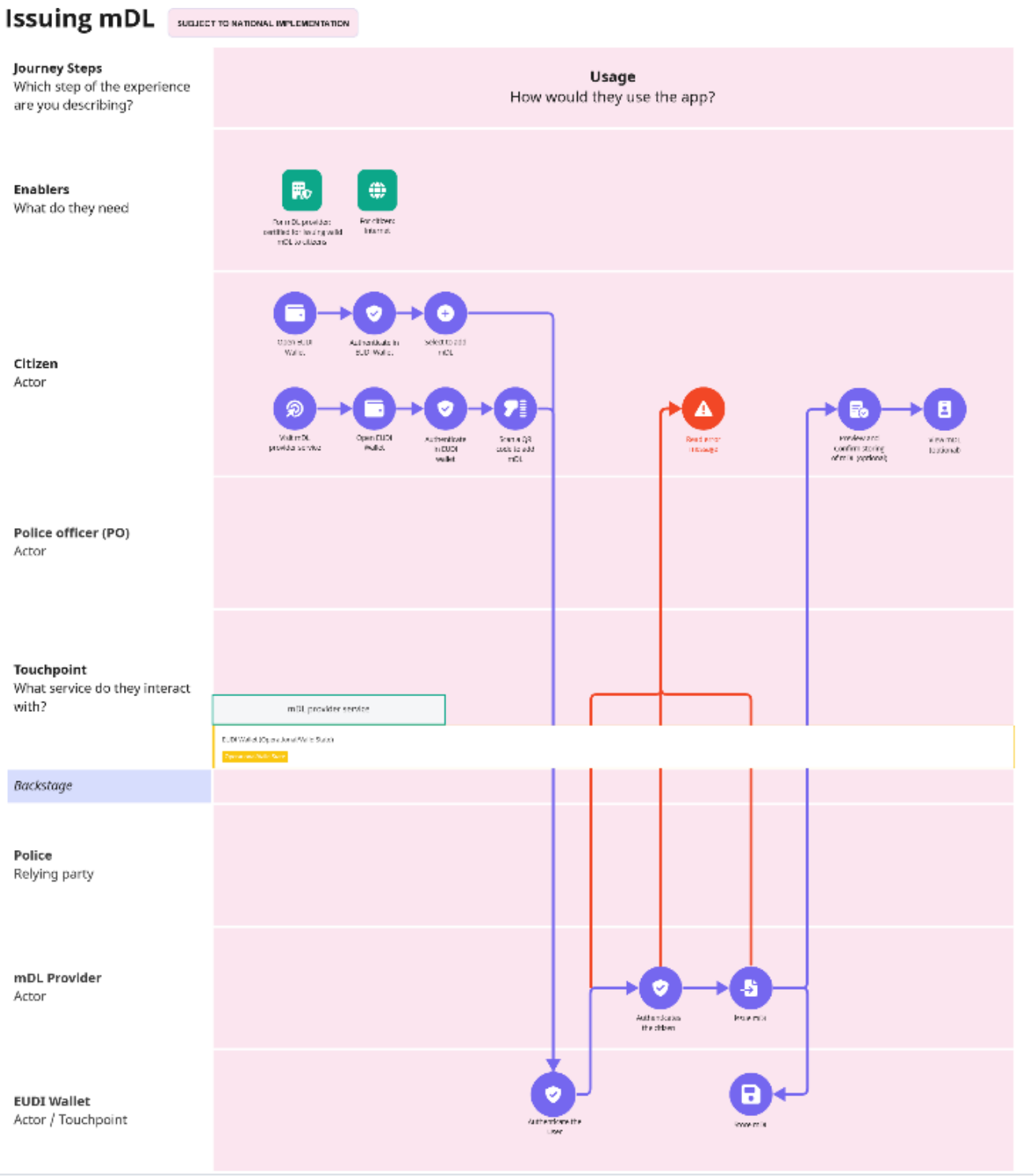
Annex 02 - identificació i autenticació en línia

El model de servei sobre identificació i autenticació en línia per a la Cartera es descriu a l'arxiu adjunt ***Annex 02- EUDI Wallet - Online Identification and Authentication.pdf***



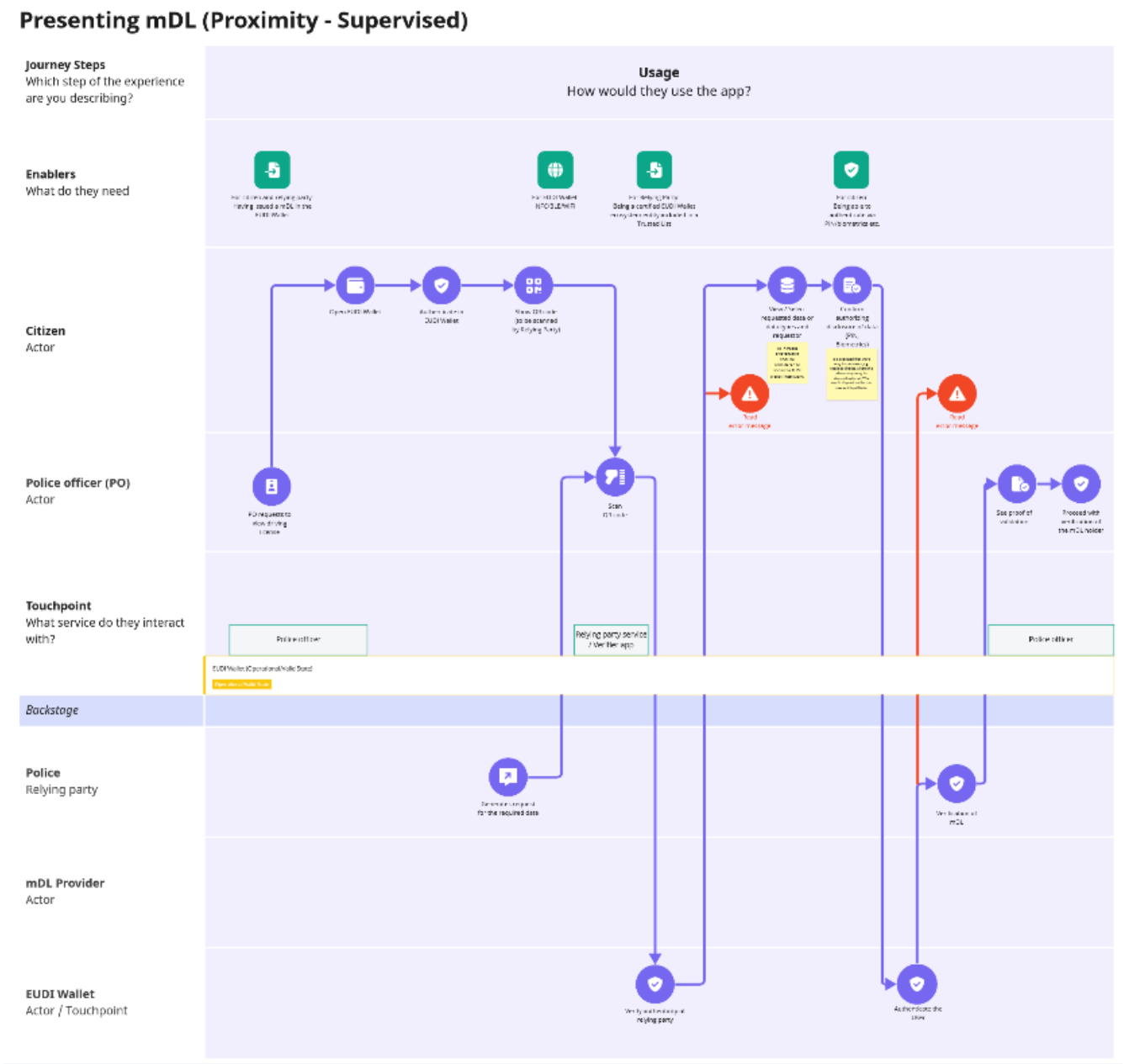
Annex 03 - Expedició de mDL

El projecte de servei sobre l'emissió de mDL es descriu a l'arxiu adjunt ***Annex 03 - EUDI Wallet - issuing mDL.pdf***.



Annex 04 - presentació de mDL (proximitysupervised)

El projecte de servei sobre la presentació ***de mDL (proximitat supervisada***) es descriu a l'arxiu adjunt ***Annex 04 - EUDI Wallet - presenting mDL (proximity-supervised).pdf***.



Annex 05 - presentació de mDL (proximityunsupervised)

El projecte de servei sobre la presentació ***de mDL (proximitat-sense supervisió***) es descriu a l'arxiu adjunt ***Annex 05 - EUDI Wallet - presenting mDL (proximity-unsupervised).pdf***.