Erreminten kutxa Batasunaren komuna, Nortasun Digitalaren Europako Esparru baterantz ikuspegi koordinatua izateko

Arkitektura eta nortasun digitaleko Europako zorroaren erreferentzia-esparrua

2023ko apirila

1.1.0 Bertsioa

DOKUMENTUAREN BERTSIOA

BERTSIO	DATA[1]	ALDAKETAK
1.0.0	2023ko urtarrilaren 26a	Lehen bertsioa
1.1.0	2023ko apirilaren 20a	Zerbitzu-planoak gehitzea erabilera-kasuetarako: - Lineako zerbitzuak eskuratzeko identifikazioa eta autentifikazioa, eta - gidabaimen mugikorra

[1] Adituen taldeak adopzio-data

Edukia

1. Sarrera

1.1. Testuingurua

2021eko ekainaren 3an, Europako Batzordeak gomendio bat onartu zuen,[2] eta bertan estatu kideei eskatzen zaie arkitektura teknikoa eta erreferentzia-esparrua (aurrerantzean, ARF,"Architecture and Reference Framework") ingelesez izendatzeagatik lan egin dezazuten tresna-kutxa bat garatzeko, arau komun eta zehaztapen teknikoen multzo bat eta jarraibide komun eta jardunbide hobeak barne.

Gomendioak zehazten duenez, emaitza horiek nortasun digitalaren Europako Esparruaren proposamena aplikatzeko oinarri izango dira[3] , eta tresna-kutxa egiteko prozesuak ez du legegintza-prozesua oztopatu edo aurrez epaituko.

Gomendioak aurreikusten du estatu kideetako adituek garatuko dutela tresna-kutxa, Batzordearekin[4]koordinazio estuan, eta, egokia denean Europar Batasuneko Nortasun Digitalaren Karterako (IDUE) azpiegituraren funtzionamendurako, sektore publiko eta pribatuetako beste alderdi interesdun batzuekin.

Gomendioan ezarritako egutegi adierazgarriari jarraituz, 2021eko irailaren 30ean lan-prozesu bat eta-prozedura batzuk adostu ziren, eta Batzordeak proposatutako IDUE Kartera ekosistemaren goi-mailako deskribapenari buruzko ofiziozko dokumentu batean eztabaidatu ziren.

Oinarri horren gainean, 2021eko urria eta abendua bitartean, IDUE zorroaren kontzeptuaren, funtzionalitateen eta segurtasun-alderdien deskribapen zehatzagoa ematen zuen eskema bat definitu zen, bai eta oinarrizko hainbat erabilera-kasu ere. Lan horrek 2022ko otsailean EIDAS Aditu Taldeak onartutako ARFaren Zirriborroa egin zuen. Eskema Futuriumen argitaratu zen[5] , publikoaren iritzia jasotzeko. Iruzkin epea 2022ko apirilaren 15ean itxi zenean, 36 alde interesatuk bidali zituzten euren iruzkinak.

Ordutik, EIDAS Adituen Taldeak Nortasun Digitalaren Europako Esparruaren kontzeptuak eta zehaztapenak garatzen jarraitu du, Batzordearen IDAS Erregelamendua berrikusteko

[2] BATZORDEAREN GOMENDIOA(EB) C(2021) 3968 amaiera, 2021eko ekainaren 3koa, Nortasun digitaleko Europako esparru baterantz ikuspegi koordinatua izateko Batasunaren tresna-kutxa erkide bati buruzkoa, EO L 210/51, 2021eko ekainaren 14koa.

[3] EIDAS Erregelamendua berrikusteari buruzko dokumentuan egindako erreferentzia guztiak Batzordearen 2021eko ekainaren 3ko proposamenari egindakotzat joko dira, kontrakorik adierazi ezean. EUROPAKO PARLAMENTUAREN ETA KONTSEILUAREN ERREGELAMENDUAREN proposamena, Europako nortasun digitalerako esparru bat ezartzeari dagokionez 910/2014(EB) Erregelamendua aldatzen duena, COM(2021) 2021eko azken 3.6.281 amaierakoa.

[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

proposamena oinarri hartuta[6], eta hala egiten jarraituko du, harik eta legegintza-negoziazioak amaitu eta betearazpen-egintzak onartu arte.

Adituen Taldeak 2023ko apirilaren 20an onartu zuen dokumentu hau.

1.2. Dokumentu honi buruz

1.2.1. Egiletza eta Lizentzia

Dokumentu hau eIDAS (eIDAS Expert Group) (E03032) Adituen Taldearen lanaren emaitza da,[7] eta azken bilera 2023/03/20an egin zen (dokumentuaren bertsio honen ondorioetarako).

Hainbat egileren lankidetza eta ekarpenak sustatzen dituen tresna batean mantentzen den dokumentu honen ingelesezko jatorrizko bertsioa eskuragarri https://code.europa.eu/eudi/architecture-and-reference-framework

Dokumentua kudeatzeko modu hori dela eta, gomendagarria da URL horretara jotzea, ingelesezko dokumentuaren bertsio eguneratuenak eskuratzeko.

Dokumentuaren Jabetza Intelektualari buruzko lizentzia Creative Commons "Atribución 4.0 Internacional (CC BY 4.0)" da , https://code.europa.eu/eudi/architecture-and-reference-framework/-/blob/main/LICENSE eta horrek aukera ematen du:

- Materiala edozein bitarteko edo formatutan kopiatu eta birbanatzea
- Materialetik egokitzea, eraldatzea eta eraikitzea, edozein helburutarako, baita komertzialki ere.

Honela geratzen da idatzita:

- Esleipena — Zuk modu egokian eman behar duzu kreditua, lizentziarako esteka bat eman, eta aldaketarik egin den adierazi. Edozein modutan egin dezakezu, baina ez zuk edo zure erabilerak lizentziaren laguntza dutela iradokitzeko moduan.

1.2.2. Itzulpena eta lizentzia.

Gaztelaniazko bertsioa **Julian Inza** EADTRUST-eko presidenteak egin du, Madrilen (Espainia) kokatutako Konfiantza Zerbitzuen Emaile Kualifikatu batek, https://eadtrust.eu webgunearekin , eta 2023ko irailaren 11n amaitu da, jatorrizko bertsioa ingelesez argitaratu eta aste batzuk

[6] EIDAS Erregelamendua berrikusteko dokumentuaren aipamen guztiak Batzordearen 2021eko ekainaren 3ko proposamenari egindakotzat joko dira, kontrakoa adierazten ez bada.
[7] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3032

geroago, Githuben webgunean.https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

Eratorritako edozein lanek adierazi behar du **Julian Inza** EADTRUST European Agency of Digital Trust, S.L.-ko presidenteak, Madrilen (Espainia) kokatutako Konfiantza Zerbitzuen Emaile Kualifikatuak, web orria https://eadtrust.eu

1.2.3. Dokumentu honen helburua.

Dokumentuaren helburua da beharrezko zehaztapen guztiak ematea IDUE zorroko konponbide elkarreragile bat garatzeko, arau eta praktika komunetan oinarritua. EIDAS Adituen Taldearen lanen egoera aurkezten du dokumentuak, eta ez du esan nahi haren edukiari edo EIS Erregelamendua berrikusteko proposamenari buruzko akordio formalik. 8. kapituluan azaltzen den bezala, dokumentu hori denborarekin osatu eta eguneratuko da, tresna-kutxa sortzeko prozesuaren bidez. Behin osatuta, dokumentuak arkitektura eta erreferentzia-esparru oso bat deskribatuko ditu, nortasun digitaleko karterako Europako soluzioa ezartzeko beharrezkoak diren zehaztapen guztiak jasoko dituena.

2-4 eta 7-8 kapituluak deskribatzaileak diren bitartean, 5 eta 6 kapituluetan DIP/PID eta TE(C) A/(Q) EAA emaileentzako eta IDUE Zorroko soluzioen inplementatzaileentzako baldintzak zehazten dira. Dokumentuan aginduzko adierazpenak RFC 2119 arau teknikoaren arabera erabiltzen dira.

Dokumentuak berak ez du balio legalik, eta ez ditu aurrez epaituko abian dagoen legegintza-prozesua eta nortasun digitaleko Europako zorroetarako nahitaezko legezko betekizunak. NORTASUN Digitalaren Europako Esparruaren proposamenaren lege-negoziazioen emaitzari egokituko zaio IFK. Azkenean onartutako Nortasun Digitalaren Europako Esparru Erregelamendua eta oinarri juridiko horren arabera onartutako betearazpen-egintzak eta delegatuak baino ez dira derrigorrezkoak izango.

1.3. Dokumentu honen erabilera

Dokumentu hori, batez ere, Europako Batzordeak erabiltzera bideratuta, IDUE Zorro baten erreferentzia-ezarpena garatzen baitu, bai eta "Large Scale Pilots" (Pilotos a Gran Escala) testuinguruan erreferentzia-ezarpenaren erabileran oinarritutako proiektu pilotuak gauzatzen dituzten partzuergoak ere. 8. kapituluaren arabera, zehaztapen hau aplikatzean lortutako esperientziak dokumentu hau hobetzea erakar dezake.

1.3.1. IDUE zorro baten erreferentzia ezartzea

Batzordeak IDUE zorroaren erreferentziazko ezarpena emango du formatu mugikor batean[8]. IDUE Zorroaren erreferentziaren ezarpenaren kodea Europa osoko inplementatzaileek berrerabiltzeko iturri irekien software gisa emango da. Lehenengo inplementatzaileak Large Scale Pilots (LSPs) proiektuak aurrera eramateko hautatutako proiektuak izango dira, lizitazio baten antzeko proposamenen deialdi baten ondoren. LSP proiektuek IDUE Zorro baten erreferentziaren ezarpenaren garapenean parte hartuko dute. Batzordeak, halaber, IDUE Zorroaren erreferentzia-ezarpenaren funtzionamendurako beharrezkoak diren zerbitzu zentralak ere emango ditu hasiera batean.

Batzordeak IDUE Zorroaren erreferentziazko aplikazioa garatzeko ARF erabiltzea proposatzen du.

1.3.2. Eskala handiko pilotuentzako orientabideak (Large Scale Pilots LSP)

IDUE zorro baten erreferentzia-ezarpena garatzen laguntzeko eta proiektu pilotuetan lehentasunezko erabilera-kasuen bidez erabiltzen direla frogatzeko, Batzordeak proposamen-deialdi bat egin zuen 2022ko otsailaren 22an, IDUE zorrorako eskala handiko erabilera-kasuak hartzeko Europa Digitalaren Programaren esparruan.

Large Scale Pilots (LSP) deialdiaren helburua da IDUE zorroa IDUE zorroa erabiliko duten proiektu pilotuak kofinantzatzea, IDUE zorroaren erreferentziazko inplementazioan oinarrituta, kontuan hartuta proiektuaren berezitasunak, jakinarazitako Nortasun Digitaleko sistemak (Adibidez, NANe Espainiaren kasuan) eta Zorroa sistemen garapen nazionalak eta inplementazio-egoerak, alderdi interesatuak, publikoak zein pribatuak, inplikatzen dituzten mugaz gaindiko erabilera-kasuen inguruan.

ARF-a LSPek erabiliko dute pilotuen sistemen diseinua eta arkitekturaren garapena informatzeko eta gidatzeko, erreferentziazko inplementazioaren argitalpenarekin batera.

Espero da LSPk IFKri buruzko iruzkinak egitea, konfiantza-alderdien zerbitzuekin, TE(C)A/(Q)EAA atributuen testigantza elektronikoen hornitzaile kualifikatuekin edo kualifikatu gabeekin, pertsonak identifikatzeko datuen hornitzaileekin (DIP/PID) eta transakzio esanguratsuen erabiltzaileekin harremanetan jarri ahala, proposatutako erabilera-kasuen arabera.

[8] Gaur egun, 2023ko bigarren hiruhilekorako lehen bertsioa aurreikusi dute, eta beste batzuk ere bai.

2. Definizioak

EIDAS (aurreko 910/2014 EB Erregelamendua) Erregelamenduaren lege-testua aldatzeko proposamenaren 3. artikuluaz gain, honako definizio hauek eskaintzen dira arkitekturarako eta erreferentzia-esparrurako garrantzitsuenak nabarmentzeko edo aipatutako lege-testuan definitu gabeko termino gehigarriak sartzeko (*)

Atributua	**Pertsona fisiko edo juridiko baten edo erakunde baten ezaugarria, ezaugarria edo ezaugarria, elektronikoki. - *EIDAS Erregelamendua aldatzeko proposamena.***
Benetako iturria	**Gordailua edo sistema, sektore publikoko organismo baten edo erakunde pribatu baten erantzukizunpean mantendua, pertsona fisiko edo juridiko bati buruzko atributuak dituena eta informazio horren lehen iturritzat hartzen dena edo estatuko legerian benetakotzat hartzen dena. - *Proposamena: EIDAS Araudia***
Atributuen testigantza elektronikoa (TEA)	*Ingelesez: Electronic Attestation of Attributes (EAA)* **Atributuak kautotzeko aukera ematen duen testigantza elektronikoa - *EIDAS Araudia***
*Jaulkitzailea**	**Pertsona identifikatzeko datuei buruzko informazioa ematen duen emaile bat (DIP/PID) edo TE(C) A/(Q)EAA atributuak jaulkitzen dituen konfiantza-zerbitzuen emaile bat (kualifikatua izan ala ez). IDUE zorroaren kasuan, DIP/PID eta TE(C) A/(Q) EAAko hainbat igorle egon daitezke.**
Egiaztapenerako erakunde nazionalak (ONA).*	*Ingelesez: National Accreditation Bodies (NAB)* **Egiaztatzeko Erakunde Nazionalak (ONA) 765/2008(EE) Erregelamenduaren arabera, Estatutik eratorritako agintaritza duten Konformazioa Ebaluatzeko Organismoak egiaztatzen dituzten estatu kideetako erakundeak dira.**
Pertsona identifikatzeko datuak (DIP)	*Ingelesez: Person Identification Data (PID)* **Pertsona fisiko edo juridiko baten edo pertsona juridiko bat ordezkatzen duen pertsona fisiko baten nortasuna ezartzeko aukera ematen duten datuen multzoa - *Erregelamendua.***
*Pertsonak identifikatzeko datuen hornitzailea**	**Erabiltzaileei lehen mailako iturri gisa identifikatzen dizkien estatu kide edo erakunde juridikoa.**

*Gako publikoaren azpiegitura (PKI)**.	*Ingelesez, Public Key Infraestructure (PKI)* **IDUE Zorro bateko osagaiek gako publikoak banatu, kudeatu eta kontrolatzeko erabiltzen dituzten sistemak, softwarea eta komunikazio-protokoloak deklaratzen ditu. PKI batek ziurtagirietan bildutako gako publikoak ematen ditu eta bere fidagarritasuna kudeatzen du, eman dituen ziurtagirien indarraldiari erantzunez.**
Atributuen testigantza elektroniko kualifikatuen emailea	**Konfiantzazko zerbitzuen hornitzaile kualifikatua, atributuen testigantza elektronikoak ematen dituena eta V. eranskinean ezarritako baldintzak betetzen dituena. - *EIDAS Erregelamendua aldatzeko proposamena***
Gailua Kualifikatua Sortzea Sinadura (DCCF)	*Ingelesez, Qualified Signature creation Device (QSCD)* **II. eranskinean ezarritako baldintzak betetzen dituzten sinadura elektronikoak sortzeko softwarea edo hardwarea.*EIDAS Araudia eta IDAS Araudia aldatzeko proposamena***
Konfiantzazko zerbitzuen emaile kualifikatua (PCSC)	*Ingelesez, Qualified Trust Service Provider (PCSC)* **Konfiantza-zerbitzuen hornitzaile bat, kualifikatutako konfiantza-zerbitzu bat edo batzuk ematen dituena, gainbegiratze-erakundeak kualifikazio-izaera eman dionean. - *EIDAS araudia***
Konfiantza duen zati bat Informatutako zatia*	**Identifikazio elektronikoan edo konfiantzazko zerbitzu batean konfiantza duen pertsona fisiko edo juridikoa . - *EIDen Araudia*** **IDUE Karteraren kasuan, IDUE Karteratik datorren identifikazio elektronikoko edo atributuetako informazioa jasotzen duen zatia.**
Dibulgazio selektiboa.*	**IDUE zorroaren gaitasuna, erabiltzaileari DIP/PID edo TE(C) A/(Q)EAAetan agertzen direnen artean atributuen azpimunttua aurkezteko aukera ematen diona.**
*Konfiantza**	**Konfiantza da, hain zuzen ere, alderdi bat hirugarren erakunde batengan konfiantza izateko prest dagoen ezaugarria, akzio batzuk gauzatu eta/ edo zenbait gai eta/ edo esparruri buruzko baieztapen batzuk egin ditzala.[9].**

[9] "OASIS Trust"-en zehaztapenen arabera, [lerroan]. Eskuragarri: http://docs.oasis-open.org/ws-sx/ ws-trust/ v1.4/ ws-trust.html.

*Konfiantza-esparrua**	**Parte-hartzaileen komunitate baten artean transakzio mota jakin batzuk egiteko diseinatutako esku-hartze ugariko sistema arautzen duten arau eta akordio operatibo eta teknikoen multzoa juridikoki eska daitekeena, eta baldintza-multzo komun bati lotuta dagoena.**
*Konfiantza-eredua**	**IDUE Zorroaren ekosisteman esku hartzen duten osagaien eta erakundeen zilegitasuna bermatzen duten arauen multzoa.**
Konfiantza-zerbitzuen hornitzailea (PSC)	*Ingelesez, Trust Service Provider (TSP)* **Konfiantza-zerbitzu bat edo batzuk ematen dituen pertsona fisiko edo juridikoa, dela konfiantza-zerbitzu kualifikatuen emaile gisa, dela kualifikatu gabeko konfiantza-zerbitzuen emaile gisa. -** ***eIDAS Erregelamendua.***
Konfiantza zerbitzua	**Aldez aurretik ordainduta ematen den zerbitzu elektronikoa, hau da:** **(a) sinadura elektronikoak eta zigilu elektronikoak babesten dituzten ziurtagiri elektronikoak sortzea, egiaztatzea eta balioztatzea, denbora elektronikoko zigiluak ematea, entrega elektroniko ziurtatuko zerbitzuak ematea eta atributuen testigantza elektronikoko zerbitzuak ematea;** **(b) web guneak kautotzeko ziurtagiriak sortu, egiaztatu eta baliozkotzea;** **(c) sinadura elektronikoak edo zigilu elektronikoak dituzten dokumentu elektronikoak gordetzea;** **(d) dokumentu elektronikoen artxibo elektronikoa;** **(e) sinadurak eta zigilu elektronikoak sortzeko urruneko gailuen kudeaketa, titularraren kontrolpean, gako pribatuak eta ziurtagiriak erabiliz;** **(f) kontabilitate elektronikoko erregistro baten antzeko mugimenduen eguneroko liburu batean datu elektronikoak erregistratzea. -** ***EIDAS Araudia aldatzeko proposamena***
*Konfiantza-zerrenda**	**Agintaritza duten erakundeei buruzko informazioa lege- edo kontratu-testuinguru jakin batean gordailutzea, egungo egoera historikoari buruzko informazioa ematen duena. Konfiantza-zerrendak era ezberdinetan ezagut daitezke.**
*Erabiltzailea**	**IDUE Kartera erabiltzen duen pertsona fisiko edo juridikoa da.**
*Zorroa eskabidea IDUE**	**Erabiltzaile baten IDUE Zorroaren Konponbidea eskabidetzea, haren kontrolpean dagoena.**

*Zorro-hornitzaileak IDUE**	**Erakunde publikoa edo pribatua, IDUE zorro-zorroaren funtzionamenduaren arduraduna, EIDEkin bateragarria, eta, adibidez, instalatu eta inizializazio bidez eska daiteke.**
Kartera irtenbidea IDUE.*	**IDUE zorro-zorroaren soluzio bat IDUE zorro-hornitzaile baten jabetzako produktu eta zerbitzuen multzoa da, konponbide horren erabiltzaile guztiei eskaintzen diena. IDUE Kartera baten soluzio bat IDUErekin bat dator CAB batek ziurtatu dezake.**

1. taula. Definizioak

** EIDAS Erregelamenduaren 3.artikuluko definizioez edo aldatzeko proposamenez gain.*

3. EUDI zorroa erabiltzeko kasuak

IDUE (EUDI Wallet) Zorroaren zehaztapenen garapena erabilera-kasuek zuzentzen dute, eta, aldi berean, IDUE Zorroaren balio-proposamena eta enpresa-betekizunak jasotzen dituzte. Horretarako, IDUE Kartera erabiltzen den kasu bakoitzerako zerbitzu-ereduak sortzen hasi da. Eskema horiek erabiltzaileei zerbitzu bat ematen parte hartzen duten osagaien eta prozesuen irudikapen bisualak dira, eta hobekuntza-eremu posibleak identifikatzeko, erabiltzailearen esperientzia optimizatzeko eta zerbitzua arintzeko tresna gisa balio dute. Eskema horiek erabilera-arau eta zehaztapen komunak ezartzeko oinarri gisa balio dute erabilera-kasu guztietarako.

Erabilera-kasuaren zerbitzu-eskemak eranskinetan daude, erantsitako dokumentu gisa. Garrantzitsua da aipatzea zerbitzu-eskemek erabilera-kasu bakoitzerako konponbide bideragarria eskaintzen dutela, baina badaude alternatibak eta aukerako urratsak. Adibidez, erabiltzaileak baimena eman dien datuak erakustea aukerakoa izan daiteke. Gainera, erabiltzailearen ibilbideak (user journeys) aldatu egin daitezke aukeratutako inplementazio-ikuspegiaren arabera, hala nola atributuen biltegiratze asakronoa edo berreskurapen sinkronoa. Horrek eragina izan lezake datuak berreskuratzeko eta partekatzeko baimena ematean.

EIDAS Adituen Taldeak zerbitzu-eskemak deskribatu ditu hurrengo erabilera-kasuetarako.

3.1 Lineako zerbitzuak eskuratzeko identifikazioa eta autentifikazioa

IDUE Karteraren helburu nagusia da linea publiko eta pribatuko zerbitzuetarako aseguramendu-maila handia duten erabiltzaileen identifikazio eta autentifikazio segurua eskaintzea (Level of Assurance, LoA). Funtsezko funtzionaltasun horrek bermatzen du alderdi informatuek segurtasunez egiaztatu ahal izango dutela pertsona zuzenarekin elkarrera eragiten ari direla.

Kasu honetan, erabiltzaileak IDUE Kartera erabiltzen du bere nortasuna baieztatzeko. Maiz sartzen da autentifikazioa eskatzen duten lineako zerbitzuetara, eta gaur egun hainbat metodo erabiltzen ditu zerbitzu horiek eskuratzean haien nortasuna egiaztatzeko. Erabiltzaileak, halaber, sareko interakzioetan identifikazio pertsonaleko datuak (PID) partekatzea ere kezkatzen du. Bere helburuen artean, erabiltzailea identifikatzea eta datu pertsonalak trukatzeko kontrola mantentzea eskatzen duten zerbitzuekin identifikatzea dira.

Erabilera-kasu honek IDUE Karterako bizi-ziklo osoa hartzen du bere baitan, erabiltzailearen ikuspuntutik, baliozko zorro bat lortu eta erabiltzailea lineako zerbitzu baten barruan identifikatu eta autentifikaziora arte. Gaur egungo deskribapena gailu beraren urrutiko fluxu bideragarri batean oinarritzen da (ikus 6.4 atala), non pertsona fisiko batek gailu mugikor bakarra erabiltzen duen, bai saioa sekurizatzeko, bai zerbitzuaren informazioa eskuratzeko.

3.2 Gidabaimen mugikorra

IDUE Karterako erabilera esanguratsuko kasu bat da erabiltzaileei dokumentu digital bat erosi, gorde eta erakustea, hala nola gidabaimen mugikorra (Movile Driving License, mDL) gidatzeko gaikuntza frogatzeko. Kasu honetan, erabiltzaileak IDUE Kartera erabiltzen du hirugarren bati baimena emateko, polizia agente gisa.

Erabilera-kasuaren deskribapena ikuskatutako eta gainbegiratu gabeko hurbiltasun-fluxuetan oinarritzen da, erabiltzailea alderdi informatu batetik fisikoki gertu dagoen eszenatokiak inplikatzen baitituzte, eta mDL atributuen trukea eta zabalkundea hurbiltasun-teknologiak erabiliz gertatzen da (adibidez, NFC, Bluetooth). Hurbileko bi fluxuek alde esanguratsua dute: *gainbegiratutako* fluxuan, IDUE Karterako mDL atributuak giza alderdi informatu bati aurkezten dizkio edo gainbegiratu egiten ditu (gailu baten laguntzarekin);

3.3. Beste erabilera-kasu batzuk

Dokumentu honen ondorengo bertsioetan, honako erabilera-kasu hauek zerbitzu-eredu gisa zehaztuko dira:

- *Osasun*

Osasun-datuetarako sarbide erraza erabakigarria da, bai testuinguru nazionaletan, bai mugaz gaindiko testuinguruetan. IDUE Kartera horrek pazientearen fitxara, errezeta elektronikoetara eta abarretara sartzeko aukera eman dezake.

- *Lanbide-prestakuntza eta-kualifikazioak*

Kualifikazioak baliozkotzeko prozeduretarako dokumentuak ematea garestia izan daiteke, eta denbora asko eraman diezaieke azken erabiltzaileei, enpresei eta enplegatzaileei, hezkuntza- eta prestakuntza-hornitzaileei eta beste erakunde akademiko batzuei. Adibidez, diploma-testigantza digitalak mugaz gaindiko moduan aurkez daitezke, beste hezkuntza- edo prestakuntza-erakunde bati edo balizko enplegatzaile bati formatu egiaztagarri, fidagarri eta kontsumigarrian. IDUE zorroak hezkuntza-kredentzial digitalak jasotzeko aukera ematen du, Atributuen Testigantza Elektronikoen bidez, ikasleek bildu eta aurkez dezaten erraztuz.

- *Finantza digitalak*

IDUE zorroak finantza-inguruneetan bezeroaren autentifikazio indartuko betekizunak betetzea erraztuko du. Batzordearen Ordainketa Txikizkarien Estrategiarekin bat etorriz[10], erabilera-kasua koordinazio estuan garatuko da estatu kideek txikizkako ordainketei buruz eta finantza-sektoreari buruz egiten dituzten aholku-taldeekin.

[10] Batzordeak Europako Parlamentuari, Kontseiluari, Europako Ekonomia eta Gizarte Komiteari eta Eskualdeetako Komiteari jakinaraztea, COM/2020/592 azken EBrako txikizkako ordainketa-estrategiari buruz.

- *Bidaiaren kredentzial digitala*

IDUE Kartera horrek bidaia-kredentzial digitalak gorde ditzake, erabiltzaileei bidaia arinagoak egiteko aukera ematen dietenak.

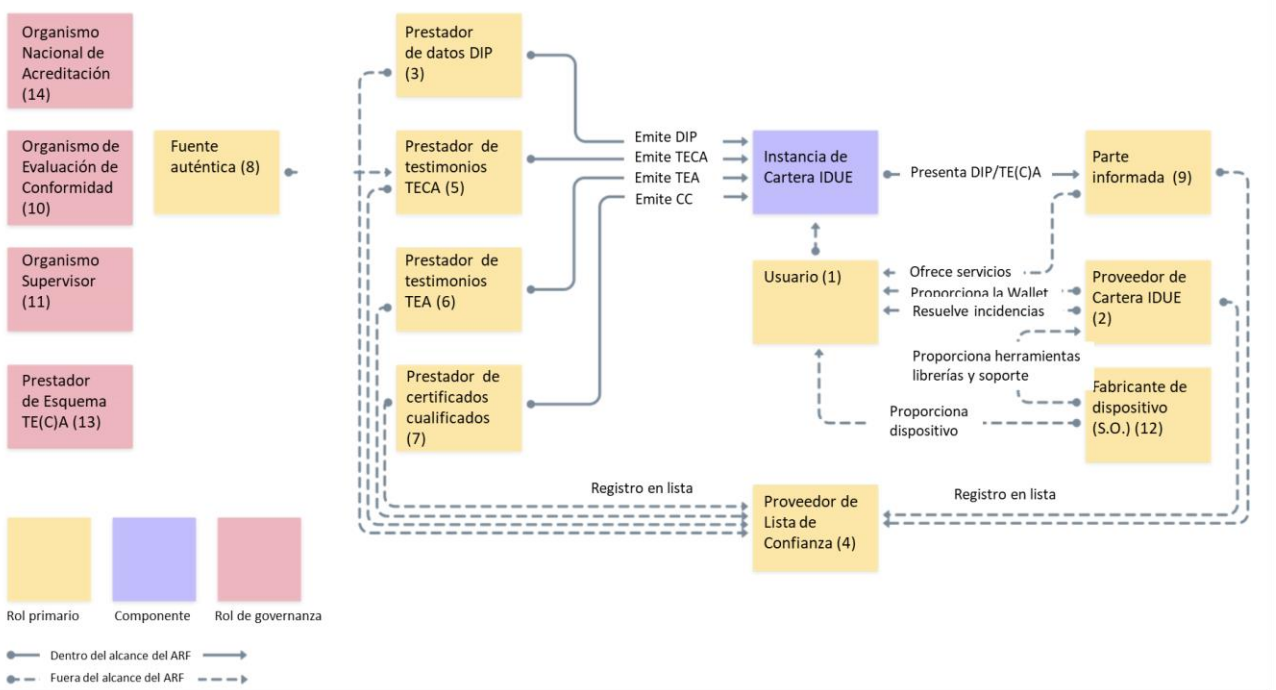
Lan hori etorkizunean beste erabilera-kasu batzuetara zabaldu ahal izango da.

4. Nortasun digitaleko zorroen Europako ekosistema

Kapitulu honek IDUE Zorroaren ekosistema deskribatzen du, Europako Batzordearen lege-proposamenean aurreikusita dagoen bezala, EB 910/2014 Erregelamendua erreformatzeko.

4.1. Ekosistemako funtzioak

IDUE Kartera ekosistemaren funtzioak 1 Irudian deskribatzen dira eta hurrengo ataletan zehazten dira.



1. irudia: IDUE zorroaren funtzioen ikuspegi orokorra

1. *IDUE Zorroen azken erabiltzaileak*
2. *Zorroen hornitzaileak IDUE*
3. *Pertsonak Identifikatzeko Datuen Hornitzaileak*
4. *Konfiantza zerrenden hornitzaileak*
5. *Atributuen testigantza elektroniko kualifikatuen hornitzaileak (TECA/QEAA)*
6. *Atributuen testigantza elektroniko ez kualifikatuen hornitzaileak (TEA/EAA)*
7. *Sinadura elektronikoko/zigilu elektronikoko ziurtagirien hornitzaile kualifikatuak edo kualifikatu gabeak*
8. *Benetako iturriak*
9. *Alderdi informatuak*
10. *Egokitasuna Ebaluatzeko Erakundeak (OEC)*
11. *Gainbegiratze-erakundeak*
12. *Erlazionatutako azpisistemen fabrikatzaileak eta hornitzaileak*
13. *TEA/ EAA edo TECA/ QEAA testigantzen eskemak*
14. *Egiaztapenerako estatu mailako organismoak*

4.1.1. IDUE Zorroaren erabiltzaileak

IDUE Zorroen erabiltzaileek IDUE Kartera erabiltzen dute beren buruari buruzko testigantzak jasotzeko, gordetzeko eta aurkezteko (DIP/PID, TECA/QEAA edo TEA/EAA), baita beren nortasuna frogatzeko ere. Erabiltzaileek Sinadurak eta Zigilu Elektroniko Kualifikatuak (QES) sor ditzakete IDUE zorroa erabiliz.

Legeria nazionalaren arabera, IDUE zorro baten erabiltzailea nor izan daitekeen zehazten da. IDUE zorro bat erabiltzea ez da derrigorrezkoa herritarrentzat, EIDAS Erregelamendua berrikusteko proposamenaren arabera. Hala ere, estatu kideak behartuta daude herritarrei IDUE zorroa emateko irtenbide bat eskaintzera.

4.1.2. Zorroen hornitzailea IDUE

IDUE zorro-hornitzaileak estatu kideak edo IDUE zorroa azken erabiltzaileen esku jartzen duten estatu kideek baimendutako edo aitortutako erakundeak dira. Estatu kide bakoitzari dagokio agintaldiaren edo aitorpenaren baldintzak zehaztea.

IDUE Zorroen Hornitzaileek IDUE Karterako Soluzio baten bidez, EIDAS Erregelamendua berrikusteko proposamenean aurreikusitako konfiantzazko hainbat produktu eta zerbitzuren konbinazio bat jartzen dute Erabiltzaileen eskura, erabiltzaileari Pertsona Identifikatzeko Datuen erabileraren gaineko erabateko kontrola ematen diotenak (DIP/PID) eta Atributu Kualifikatuen edo Kualifikatu gabekoen testigantza elektronikoak (TECA/QEAA edo TEA/EAA), eta IDUE Karterako beste edozein datu pertsonal. Ikuspegi tekniko batetik, horrek esan nahi du, halaber, erabiltzaileari bermatu ahal izango diola zenbait agertokitan datu horiek erabiltzearekin lotutako material kriptografikoaren gaineko kontrol esklusiboa(adibidez, gako pribatuak), identifikazio elektronikoa barne, edo sinadurak edo zigilu elektronikoak egitea.

IDUE zorro-hornitzaileak IDUE zorroetarako baldintzak betetzen direla bermatzeaz arduratzen dira.

4.1.3. Pertsona identifikatzeko datuen hornitzaileak (DIP/PID)

DIP/ PID hornitzaileak honako hauen ardura duten konfiantzazko erakundeak dira:

- IDUE Zorroaren erabiltzailearen nortasuna egiaztatzea, Goi-mailako Aseguramendu Maila (LoA high) ezarritako baldintzen arabera.
- IDUE Zorroari DIP/ PID ematea, formatu komun bateratuan, eta
- informazioa ematea[11], alderdi informatuek DIP/ PIDren baliozkotasuna egiazta dezaten.

Estatu kide bakoitzari dagokio zerbitzu horien baldintzak zehaztea.

DIP/ PID hornitzaileak izan daitezke, adibidez, gaur egun nortasun-agiri ofizialak, nortasun-bitarteko elektronikoak, IDUE zorro-hornitzaileak eta abar ematen dituzten erakunde berberak. IDUE zorro-hornitzaileak DIP/ PID hornitzaileen erakunde berak izan daitezke edo ez.

4.1.4. Konfiantzazko zerrenden hornitzaileak

[11] Informazioa ematen duen mekanismo zehatza alde batera utzi gabe, zuzenean edo zeharka

IDUE Kartera ekosisteman rol baten estatus espezifikoa modu fidagarrian egiaztatu ahal izango da. Hauek dira rol horiek:

- Zorro-hornitzaileak IDUE
- Pertsonak Identifikatzeko Datuen Hornitzaileak
- Atributu kualifikatuen testigantza elektronikoen hornitzaileak (TECA/QEAA)
- Sinadura eta zigilu elektronikorako ziurtagiri kualifikatuen hornitzaileak (CC/QC)
- Alderdi informatuak (batzuetan, Konfiantza duten alderdiak)
- Atributuen testigantza elektronikoen hornitzaile ez kualifikatuak (TEA/EAA)
- Sinadura eta zigilu elektronikoetarako kualifikatu gabeko ziurtagirien hornitzaileak
- Konfiantzazko beste zerbitzu batzuen hornitzaileak
- Atributuen eta Eskemen katalogoak atributuen testigantza-hornitzaileentzat

Beste funtzio batzuk beharrezkoak izan daitezke, eta, beraz, berariazko funtzioaren eta kritikotasunaren arabera definitu eta aipatu behar dira esplizituki, adibidez, urrutiko sinadura-prozesuetan parte hartzen duten funtzio eta eragileen arabera.

Erabiltzen denean, Konfiantza-zerrenda batek [12] mekanismo bat izan behar du, erakunde fidagarriei buruzko informazioa erakunde fidagarriei buruzko informazioa sartu edo kentzeko, erakunde horien erregistroa mantenduz eta hirugarrenei informazioa emanez. Konfiantza-zerrenda bat kudeatzen duen erakunde bakoitzari dagokio(erregistratzailea) entitateek zerrendan aipatzeko bete behar dituzten baldintzak ezartzea, lehendik dagoen araudi batek, adibidez, araudi sektorialean aurrez zehaztuta daudenean.

4.1.5. Atributuen testigantza elektroniko kualifikatuaren hornitzaileak

TEA/EAA testigantzak PCSCk ematen ditu (Konfiantza Zerbitzuen Emaile Kualifikatuak, ingelesez QTSP, Qualified Trust Service Providers). PCSCetarako konfiantza-esparru orokorra TEKA/QEAEi ere aplikatzen zaie, baina konfiantza-zerbitzu horretarako arau espezifikoak zehaztea ere beharrezkoa da. TECA/QEAAko hornitzaileek interfaze bat dute TECA/QEAA eskatzeko eta emateko, IDUE zorroekin elkarrekiko autentifikazio-interfazea barne, eta, ahal bada, benetako iturriekiko interfazea, atributuak egiaztatzeko. TECA/QEAAko hornitzaileek TECA/QEAAren baliozkotasun-egoerari buruz galdetzeko erabil daitezkeen zerbitzuen informazioa edo kokapena ematen dute, testigantzen erabilerari buruzko informaziorik jaso ezinik. PCSC bakoitzari dagokio zerbitzu horien baldintzak eta baldintzak zehaztea, IDAS Erregelamenduan zehaztutakoa baino gehiago.

4.1.6. Atributuen testigantza elektroniko ez kualifikatuaren hornitzaileak

[12] Aurrerago, konfiantza-zerrendak nola aplika daitezkeen zehaztuko da.

Kualifikatu gabeko TEA-ak konfiantza-zerbitzuen hornitzaile kualifikatuek edo kualifikatu gabeek eman ditzakete. EIDASen arau-esparruaren arabera gainbegiratuta dauden arren, pentsa daiteke EIDASaz bestelako beste esparru juridiko edo kontratu-esparru batzuek, gehienbat, lehendik dauden TEA-ak emateko, erabiltzeko eta aitortzeko arauak arautzen dituztela.

Beste esparru horiek politika-arloak har ditzakete, hala nola gidabaimenak, hezkuntza-kredentzialak edo ordainketa digitalak, baina atributuen testigantza elektronikoko hornitzaile kualifikatuetara ere jo dezakete. TEA erabiltzeko, PSC/TSPek TEA eskatzeko eta lortzeko modu bat eskaintzen diete erabiltzaileei, eta horrek esan nahi du teknikoki bete behar dituztela IDUE Zorroaren interfazearen zehaztapenak. Jabari-arauen arabera, TEA/ EAA hornitzaileek TEA/ EAAren baliozkotasunari buruzko informazioa eman dezakete, alderdi informatuak TEA/ EAA-en erabilerari buruzko informaziorik jasotzeko aukerarik izan gabe. TEA jaulkitzeko baldintzak eta lotutako zerbitzuak arau sektorialen mende daude.

DIP/PID, TEA/ EAA eta TECA/QEAA emaile kualifikatu eta kualifikatu gabeek ere **alderdi informatzaile** izena jaso dezakete, jasotzen dituzten lekukotasunetan *konfiantza duten alderdiekin* kontrastean, eta **alderdi informatuak** ere deitzen dira.

4.1.7. Sinadura eta zigilu elektronikoetarako Ziurtagiri Kualifikatuen eta Ez Kualifikatuen emaileak

EIS Erregelamendua aldatzeko proposamenak jasotzen duen"COM(2021)281 azken" izeneko testuaren 6 bis artikuluaren 3 paragrafoak eskatzen du IDUE zorroak erabiltzaileari sinadura edo zigilu elektroniko kualifikatuak sortzeko aukera ematea. Helburu hori hainbat eratara lor daiteke:

- IDUE zorroa sinadura edo zigilua sortzeko gailu kualifikatu gisa ziurtatuta (DCCF edo DCCS, ingelesez Qualified Signature/Seal Creation Device, QSCD), edo
- Sinadura/ zigilua egiteko autentifikazio- eta inbokazio-ahalmen seguruak inplementatzen ditu, tokiko DCCF/ QSCD baten edo PCCF/QSCD urruneko baten zati gisa, PCSC/ QTSP batek kudeatua.

IDUE Zorroaren eta DCCF/QSCD-en arteko interfazeak ARF dokumentu honen etorkizuneko bertsioetan zabalduko dira.

4.1.8. Konfiantzazko beste zerbitzu batzuen hornitzaileak

IDUE Karterako interakzioa konfiantzazko beste zerbitzu kualifikatu edo kualifikatugabe batzuen hornitzaileekin, hala nola denbora-zigiluekin, xehetasun handiagoz deskribatu ahal izango da ARF dokumentu honen etorkizuneko bertsioetan.

4.1.9. Benetako iturriak

Benetako iturriak legeak aitortu edo eskatzen dituen gordailu edo sistema publiko edo pribatuak dira, pertsona fisiko edo juridiko baten gaineko atributuak dituztenak. VI. eranskinaren eremuan, EIDAS Erregelamendua berrikusteko proposamenaren eremuan benetako iturriak honako hauei buruzko atributu-iturriak dira: zuzendaritza, adina, sexua, egoera zibila, familia-osaera, nazionalitatea, hezkuntza- eta prestakuntza-tituluak eta-lizentziak, lanbide-kualifikazioen tituluak eta lizentziak, baimen eta lizentzia publikoak, finantza- eta enpresa-datuak. VI. eranskinaren aplikazio-eremuan sartzen diren iturri autentikoek interfazeak eman behar dizkiete TECA/QEAA hornitzaileei, aipatutako atributuen benetakotasuna egiaztatzeko, dela zuzenean, dela nazio-mailan aitortutako bitartekari izendatuen bidez. Benetako iturriek TE(C)A/(Q) EAA testigantzak ere eman ditzakete, eIDAS Erregelamenduaren baldintzak betetzen badituzte . Estatu kideei dagokie zerbitzu horiek emateko baldintzak eta baldintzak zehaztea , baina atributuen testigantza elektroniko kualifikatuak egiaztatzeko prozedurei aplikatu beharreko zehaztapen tekniko, arau eta gutxieneko prozeduren arabera.

4.1.10. Alderdi Informatuak (edo konfiantza duten alderdiak)

Alderdi Informatuak pertsona fisiko edo juridikoak dira, eta identifikazio elektronikoan edo konfiantzazko zerbitzu batean konfiantza dute. IDUE zorroen testuinguruan, IDUE zorroen erabiltzaileen DIP/PID, TECA/QEAA eta TEA/EAA datu-multzoan jasotako atributuak eskatzen dituzte, IDUE zorroan konfiantza izateko, zorroaren jabeak aldez aurretik onartuta (erabiltzailea) eta legeriaren eta aplikatu beharreko arauen mugen barruan. IDUE zorroan konfiantza izateko arrazoia legezko betekizuna, kontratu-akordioa edo erakunde informatuaren erabakia bera izan daiteke. IDUE Kartera batetik informazioa jasotzeko, alderdi informatuek IDUE Karteretatik datorren informazioa jasotzeko asmoaren berri eman behar diote kokatuta dauden estatu kideari. Konfiantza duten alderdiek IDUE Karterarekin interfazea izan behar dute, elkarrekiko autentifikazioa duten testigantzak eskatzeko. Informatutako aldeak DIP/PID eta TE(C) A/(Q) EAAak autentikotzeaz arduratzen dira.

4.1.11. Egokitasuna ebaluatzeko erakundeak(OEC)

IDUE zorroak estatu kideek izendatutako erakunde publiko edo pribatu egiaztatuek ziurtatuta egon behar dira[13]. Egokitasuna ebaluatzeko organismoek(OEC, ingelesez, CAB, Conformity Assessment Bodies) ikuskatu behar dituzte aldizka PCSCak. OEC/CAB egiaztapenerako estatu mailako organismo batek egiaztatzen ditu, 765/2008 Erregelamenduaren arabera, estatu kideek IDUE zorro bat eman aurretik edo KonfiantzaZko Zerbitzuen Hornitzaile bati"kualifikatu" estatusa eman aurretik oinarritu beharko dituzten ebaluazioak egiteko ardura duen aldetik. OEC/CAB-ek IDUE zorroen ebaluazio/homologazio lanak egiteko erabiltzen dituzten arauak eta erregimenak aurrerago zehazten dira"Toolbox" prozesuan.

4.1.12. Gainbegiratze-erakundeak

[13] 6 quater artikulua, 3 paragrafoa

Estatu kideek Europako Batzordeari jakinarazi behar diote PCSC/QTSPak gainbegiratzea helburu duten gainbegiratze-erakundeak izendatzea, eta, beharrezkoa izanez gero, kualifikatu gabeko konfiantza-zerbitzuen hornitzaileei dagokienez jarduten dute.

4.1.13. Erlazionatzeko gailu eta erakundeen fabrikatzaileak

IDUE zorroek hainbat interfaze izango dituzte oinarri dituzten gailuekin, eta honako helburu hauek izan ditzakete:

- Tokiko biltegiratzea.
- Interneterako sarbidea linean.
- Sentsoreak, hala nola smartphone kamerak, sentsore infragorriak, mikrofonoak, etab.
- Offline komunikazio-kanalak, hala nola Bluetooth Low Energy (BLE), "WIFI Aware" teknologia, Near Field Communication (NFC).
- Pantailak, linternak, bozgorailuak, etab.
- Txartel adimendunak eta elementu seguruak (SE, smartphone-aren osagaia).

Material kriptografikoa modu seguruan biltegiratzeko, interfaze bat ezar daiteke gailu edo zerbitzu espezifikoekin. Lotutako beste erakunde batzuk zerbitzu-hornitzaileak izan daitezke, hala nola, hodeiko zerbitzuen hornitzaileak, App aplikazio-denten hornitzaileak, etab.

EIDAS erregelamendua erreformatzeko lege-proposamenak murrizketak ezartzen ditu (adibidez, Goi Mailako Aseguramendu Maila –"LoA high") IDUE Kartera jaulkitzeko erabil daitezkeen gailu eta zerbitzu motak. Era berean, lotutako gailuen interfazeen hornitzaileen eta zerbitzu-hornitzaileen erabilgarritasunak eta baldintzek beste murrizketa batzuk ezarriko dituzte IDUE zorro-hornitzaileentzat.

4.1.14. Atributu Kualifikatuen eta Kualifikatu gabekoen testigantza elektronikoen eskemak

TE(C)A/(Q) EAA eskemen hornitzaileek TE(C) A/(Q) EAA testigantzen egitura eta semantika deskribatzen duten eskemak eta hiztegiak argitaratzen dituzte. Horri esker, beste erakunde batzuek, hala nola informatutako aldeek, TE(C) A/(Q) EAAak aurkitu eta baliozkotu ahal izango dituzte. Europako Batzordeak horretarako gutxieneko zehaztapen teknikoak, arauak eta prozedurak ezartzen ditu. Eskema komunak egotea, baita erakunde sektorial espezifikoen aldetik ere, funtsezkoa da TE(C) A/(Q) EAAak oro har onartzeko.

4.1.15. Egiaztapenerako estatu mailako organismoak

765/2008(EE) Erregelamenduaren arabera, Egiaztapenerako Erakunde Nazionalak(ONA, ingelesez NAB, National Accreditation Bodies) [14] dira estatu kidetik eratorritako agintaritzarekin egiaztapena egiten duten estatu kideetako erakundeak. ONA/NABek OEC/CAB-ak egiaztatzen dituzte produktu/zerbitzuak/prozesuak ziurtatzeko ardura duten lanbide-ziurtagiriko erakunde eskudun, independente eta gainbegiratu gisa, baldintzak ezartzen dituzten arau-dokumentuak erabiliz(adibidez, legeriak, zehaztapenak, babes-profilak, arau teknikoak). ONA/NABek akreditazio-ziurtagiria eman dieten OEC/ CAB-ak gainbegiratzen dituzte.

4.2. Zorro baten bizi-zikloa IDUE

IDAS Erregelamendua erreformatzeko proposamen-testuak IDUE zorroa abstrakzio-maila handiarekin definitzen du, bai eta estatu kide bateko biztanle/egoiliarrek IDUE zorro baliodun eta erabat funtzionala lortu ahal izatea bermatzeko legezko betebeharra duten IDUE zorro-hornitzaileak ere. IDUE Kartera baten bizi-zikloak zenbait interakzio izango ditu Konfiantza Zerrenden Hornitzaileekin, IDUE Zorroen ekosisteman rol baten egoera modu fidagarrian zehazten dutenak. IDUE Kartera hori garatzeko gida gisa balio behar duten Arkitektura eta Erreferentzia Marko bat garatzeak abstrakzio-maila zehatzagoa eskatzen du, eraginkorra izateko eta arkitekturaren deskribapena preskribatzailea izateko bezain adierazkorra izan dadin.

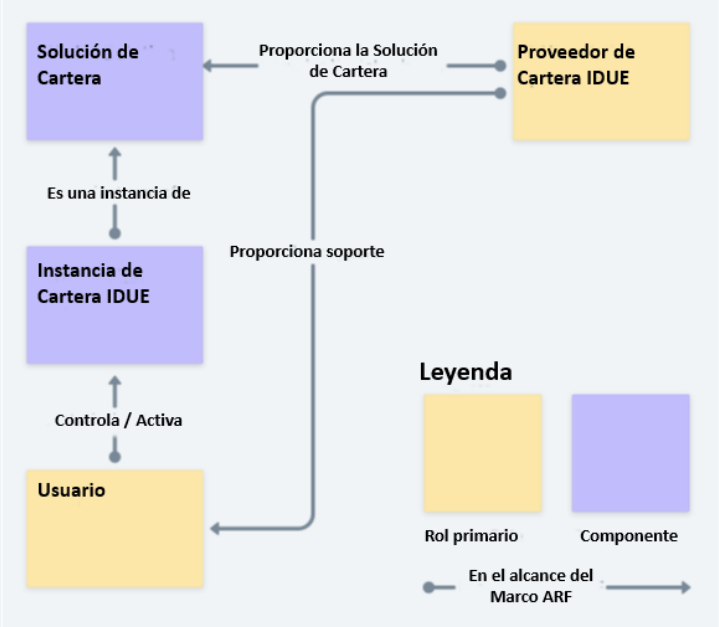
Kapitulu hau gutxieneko objektuen eredu batetik abisatzen da eta kontzeptu nagusien bizi-zikloa definitzen du: IDUE Karterako soluzioa, DIP/PID, TE(C) A/(Q) EAA eta IDUE KarteraKo Eskaera. Kontzeptu horiek abiapuntu gisa aukeratu dira, IFKren garapen bateratuak kontzeptu horien bizi-zikloak estuki elkarlotuta daudela erakutsi zuelako, eta horrek deskribapen ez oso argia eragin zuen eta, ondorioz, gaizki-ulertuak eragin zituen.

Objektuen eredua IFKren etorkizuneko bertsioetan beharrezkoa den arabera handituko da.

4.2.1. Zorroaren eredu sinplifikatua IDUE

2. irudian IDUE Zorroaren Soluzioa eta IDUE Zorroaren Eskaera kontzeptuak bereizten dira. IDUE Kartera irtenbide bat IDUE Zorroaren Hornitzaile batek emandako produktu eta/ edo zerbitzu osoa da. IDUE Karterako Instantzia bat IDUE Zorroa soluzio baten instantzia pertsonala da, bere erabiltzailearen gailu batean gauzatzen dena eta hura kontrolatzen duena.

[14] 765/2008(EE) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2008ko uztailaren 9koa, produktuen merkaturatzeari buruzko merkatua egiaztatzeko eta jagoteko betekizunak ezartzen dituena eta 339/93(EEE) Erregelamendua indargabetzen duena.



2. irudia: Zorro zorroko objektuen eredu sinplifikatua IDUE

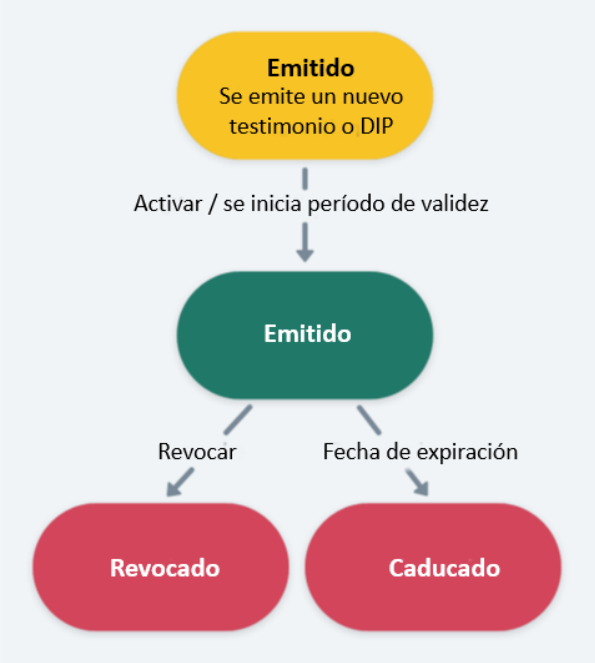
Definizio hori ez da forma-faktorearen preskriptiboa, eta, beraz, ezarpenaren arabera, IDUE Karterako Instantzia bat aplikazio mugikor bakarra izan daiteke, edo erabiltzaile jakin batentzat eskuragarri dauden tokiko eta urruneko osagai-multzo bat.

4.2.2. DIP/PID eta TE(C) A/(Q) EAA-en bizi-zikloak

DIP/PID eta TE(C) A/(Q) EAA-en bizi-zikloak funtsean berdinak dira, baina deskribapen honen irismenerako EPI bakarrik aipatuko dugu. EPIri aplikatutako atal honetako testua mutatis mutandis aplikatzen zaie TE(C) A/(Q)EAAei.

IDUE Zorroaren testuinguruan, DIP/ PID-ak bere bizi-zikloa hasten du IDUE KarteraKo Instantzia bati igortzen zaionean. Kontuan izan horrek esan nahi duela benetako iturriko atributuen kudeaketa (egitura nazionalak eta atributuen definizioak errespetatuz) IFKren eremutik kanpo geratzen dela.

Kontuan izan behar da, erabilera-kasu jakin batzuetan, DIP/ PID-ak aurrez hornituta egon daitezkeela, eta horrek esan nahi du oraindik ez direla baliozkoak igortzen direnean, baina geroago lortzen dute baliozkotasuna. DIP/ PIDak baliozkotasuna hasten den datan edo geroago jaulkitzen badira, berehala joko da egoera zuzenean aldatzen dela baliozkotzat, egiaztapen-data baliozkotasuna hasi ondorengoa bada. Horrek esan nahi du DIP/PIDak" aurre-mitituta" egon litezkeela.



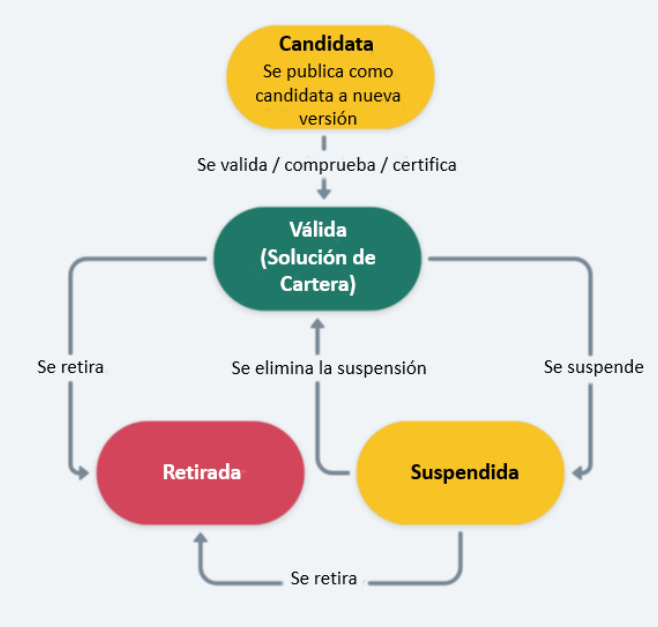
3 irudia: DIP/ PID-ren egoera-diagrama

Baliozko DIP/PID baten bi trantsizio posible daude: edo automatikoki amaitzen da,*"balio-amaierako data"* gainditzeagatik, edo hornitzaileak modu aktiboan baliogabetzen du, amaitu baino lehen. Iraungitzea eta errebokazioa funtsean independenteak diren trantsizioak dira. DIP/ PID iraungi edo baliogabetu ondoren, ezin da berriro baliozkoa izan. DIP/PID (adibidez, izen aldaketa baten ondorioz) eguneratzeko, emisio berri bat behar da beti.

4.2.3. Konponbidearen bizi-zikloa IDUE Kartera

IDUE Karterako soluzio batek egoera propioa du, etorkizuneko Erregelamenduaren 10 bis artikuluan definitzen den bezala. Konponbidearen egoerak IDUE Zorroaren Konponbide horren IDUE Zorroko instantzia guztien egoerari eragiten dio. "**Candidato"** estatua IDUE Kartera irtenbide baten lehen estatua da. Horrek esan nahi du erabat inplementatuta dagoela eta IDUE Zorroen Hornitzaileak konponbidea IDUE Zorro gisa ziurtatzea eskatzen duela.

Lege- eta irizpide tekniko guztiak bete badira, OEC/CAB-k Zorroa/Wallet konponbidearen ziurtagiria barne, orduan estatu kide batek erabaki dezake Erabiltzaileei konponbidea emateko eskaerak **ematen** hastea . Konponbidearen egoera "**baliozkoa"** da. 6 quinquies artikuluaren arabera, estatu kideak Batzordeari jakinaraziko dio bere Zorroa/Wallet soluzioaren ziurtapen-egoeran egindako edozein aldaketa. Horrek esan nahi du IDUE Karterako soluzioa **ofizialki abiarazi** daitekeela eta erabiltzaileei konponbidearen eskaerak eman dakiekeela.



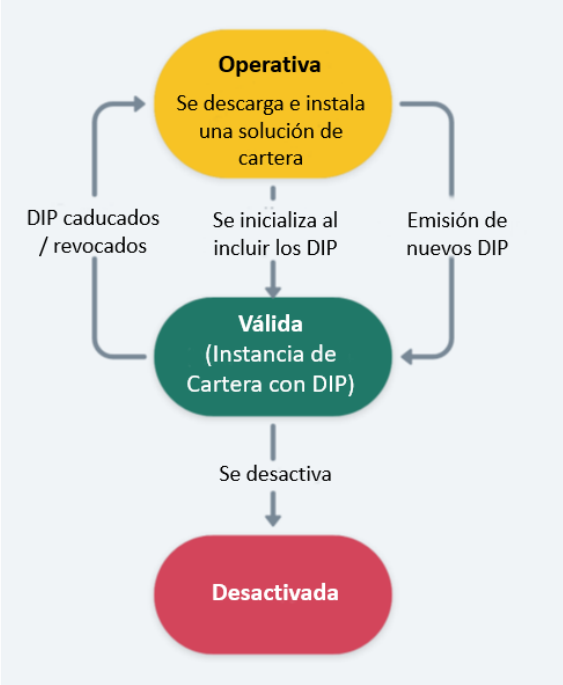
4. irudia: Cartera/ Wallet soluzioaren egoera-diagrama

10 bis artikuluaren 1 paragrafoko legezko baldintzetan, estatu kide emaileak aldi baterako eten dezake IDUE Zorroa konponbide bat. Hori, adibidez, IDUE Zorroaren konponbide horretan segurtasun arazo kritiko baten ondorioz izan daiteke. Horrek "**suspendida**" egoera ematen du. 10 bis artikuluaren 2 paragrafoaren arabera, estatu kide emaileak Zorroa/Wallet soluzioaren etendura bertan behera utzi dezake, eta jaulkipenarekin jarraitu, eta konponbidea estatu"**baldunari"** itzuli. 3. paragrafoaren arabera, IDUE Kartera soluzioa erabat kendu eta bertan behera ezezta daiteke.

4.2.4. IDUE zorro-orriaren bizi-zikloa

IDUE KarteraKo Instantzia batek bere bizitzari ekiten dio, baliozko IDUE Zorroaren Soluzio batean oinarrituta. IDUE Zorroaren Hornitzaileak IDUE Zorroaren Soluzioa ematen dio erabiltzaileari, eta, horren arabera, erabiltzaileak bere gailuan instalatu eta aktibatu ondoren, zorro-orriko instalatze bat gauzatzen du egoera" **operatiboan".** Forma-faktorearen eta inplementazioaren arabera, instantzia bat emateak hainbat ekintza eska ditzake, adibidez, IDUE mugikor bat instalatzea eta inizializatzea. Mota horretako IDUE Zorroa instantzia bat IDUEren berariazkoak ez diren eginkizunetarako erabil daiteke, hala nola fideltasun-txartelak edo pertsonalizatu gabeko tren-txartelak biltegiratzea, edo baliozko DIP/PID batzuekin loturarik eskatzen ez duen beste edozein ziurtagiri.

IDUE Zorroa instantzia bat inizializatzen denean,"baliozkotzat" jotzen da, eta horrek esan nahi du DIP/PID hornitzaile batek aintzat hartzen duela eta BALIOZKO DIP/PID multzo bat duela. DIP/PIDak iraungitzen edo baliogabetzen badira, IDUE Kartera ez da automatikoki erabiltzen, baizik eta haien egoera" operatibora" **jaitsita** . Horrek eragina izan dezake TE(C) A/(Q) EAA testigantza baten edo sinadura edo zigilu elektronikoetarako ziurtagiri kualifikatu baten baliozkotasunan.



5. irudia: Zorro-orriaren egoera-diagrama

Gaur egun, erabiltzaileak bakarrik[15] desaktibatu ahal izango du IDUE Zorroa. Kontuan izan behar da horrek ez duela zerikusirik DIP/PID datu-emaile batek edo TE(C) A/(Q) EAA testigantza-hornitzaile batek bere testigantzak bertan behera ustiatzeko aukerarekin.

[15] Adibidez , erabiltzailea hiltzen bada edo IDUE Zorroaren segurtasunaren kalteberatasuna gertatzen bada.

5. DIP/PID eta TE(C) A/(Q) EAA egiteko baldintzak

5.1. Pertsonaren identifikazio-datuak

Kapitulu honetan IDUE Karterako DIP/ PID multzoa zehazten da.

DIP/ PID hornitzaile batek DIP/ PID datu-multzo bat jaulki dezake IDUE zorrorako, eta IDUE zorroa identifikazio elektronikorako bitarteko gisa erabiltzeko aukera eman dezake lineako eta lineatik kanpoko zerbitzuak eskuratzean.

DIP/PID sortzen duten eta IDUE Zorroari ematen zaizkion mekanismoak estatu kideen mende daude, eta lege-betekizunek bakarrik mugatuta daude, hala nola aseguru-maila (LoA High), RGPD/GDPR edo beste edozein lege nazional edo Europar Batasunekoak.

Jarraian, datuen formatua deskribatuko da, Alderdi erabiltzaileari aurkezten zaion moduan, IDUE zorroak aldez aurretik datu horiek nola berreskuratu edo sortu zituen azaldu gabe.

5.1.1 Datu-multzoa

5.1.2.1. DIP/PID multzoa berrikusteko printzipioak

Kapitulu honek eIDAS"CIR 2015/1501" arauan zehaztutako aukerako datu-multzoak berrikustea proposatzen [16] du, eta beste zehaztapen batzuk, datuen minimizazioa eta identifikatzaileak aztertzen dira.

Hemen proposatzen den aukerako datu-multzoaren berrikuspena honako printzipio hauetan oinarrituta eraikitzen da:

- Ez da bi pertsona egon behar DIP/ PID derrigorrezko atributu-multzo berarekin.
- DIP/PID multzoak, gutxienez,"CIR 2015/1501" Betearazpen Erregelamenduan zehaztutako atributuen gutxieneko multzoa jaso behar du, nahitaezkotzat hartuta.
- Nahitaezko datuen multzoa, berez, estatu kide guztiek pertsona fisiko eta juridiko guztientzat eman dezaketenaren eta identifikazio elektronikorako behar denaren elkargunera mugatzen da(rzkina).

[16] Batzordearen 2015/1501(EB) Betearazpen Erregelamendua, 2015eko irailaren 8koa, Interoperabilitate-esparruari buruzkoa, Europako Parlamentuaren eta Kontseiluaren 910/2014(EB) Erregelamenduaren–barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantza-zerbitzuei buruzkoa– 12.8 artikuluaren arabera.

5.1.1.1. Pertsona fisikoentzako DIP/ PID-aren atributuak

Hurrengo taulak gaur egun eIDAS esparruan dauden DIP/ PID atributuen eta sartzen diren aukerako atributu gehigarrien ikuspegi orokorra eskaintzen du.

Nahitaezko eIDAK	Atributuak aukerakoak	Aukerako atributu gehigarriak
Abizena(k) gaur egun	**Abizena(k) jaiotzez**	**Nazionalitatea/ Herritartasuna***
Gaur egungo izenak	**Jaiotza-izenak**	
Jaiotegun	**Jaioleku**	**Estatu-mailan erabiltzen diren aukerako atributuak, adibidez, identifikazio fiskaleko zenbakia, gizarte-segurantzaren zenbakia, etab.**
Identifikatzaile bakarra	**Egungo zuzendaritza**	
	Generoa	

2. taula - PERTSONA fisikoentzako DIP/PID-en nahitaezko eta aukerako atributuak

**Nacionalidad/Ciudadanía - balizko atributu multibalora da, herritarrek nazionalitate bat baino gehiago izan dezaketelako. Hala ere, nazionalitatea/hiritartasuna TE(C) A/(Q) EAA moduan ere komunika daiteke, herritarrek nazionalitate jakin bat frogatu ahal izan dezaten, DIP/PID multzoa eguneratu gabe eta DIP/PID hornitzailea inplikatu gabe.*

Aukerako atributu gehigarriak gehitu dira, linean zein lineatik kanpo autentifikazio-aukera gehiago emateko, bai eta EIDAS-en egungo inplementazioetatik eratorritako ikaskuntzari ekiteko ere.

DIP/PIDekin lotutako metadatuek, horrez gain, honako hauek zehaztu ditzakete: jaulkipen- eta/edo iraungitze-data, agintaritza jaulkitzailea eta/edo estatu kidea, titularraren lotura egiteko behar den informazioa eta/edo edukitza-proba, atributuen balio-egoera kontsultatzeko erabil daitezkeen zerbitzuen informazioa edo kokapena, eta informazio gehiago izan dezakete.

5.1.2 EPI emateko baldintzak

Hurrengo koadroan, ZIURTAGIRIan sartzen den informazioari dagokionez, DIP/PIDei aplikatu beharreko betekizunak zehazten dira, adibidez, baliozkotasuna, benetakotasuna, balidazioa, politikak, datu-eredua eta formatuak egiaztatzeko.

Testu honen etorkizuneko bertsioek taula handitu ahal izango dute, baldintzak zehazteko. Kontuan izan behar da baldintza horiek IDUE Zorroaren zehaztapenen lehen bertsiora bideratuta daudela, eta zehaztapenak aldatu ahala alda daitezkeela.

#	Betekizuna
1	**DIP/ PIDri buruzko testigantzak DIP/ PID hornitzailea identifikatzeko behar den informazioa jaso behar du.**
2	**DIP/ PIDri buruzko testigantzak datuen osotasuna egiaztatzeko behar den informazioa jaso behar du.**
3	**DIP/ PIDri buruzko testigantzak egiazkotasuna egiaztatzeko behar den informazioa jaso behar du.**
4	**DIP/ PIDri buruzko testigantzak testigantzaren baliozkotasun-egoera egiaztatzeko behar den informazio guztia jaso behar du.**
5	**DIP/PIDri buruzko testigantzak alderdi informatu batek titularraren lotura egiaztatzeko behar duen informazio guztia jaso behar du(atributu gisa edo sinatutako beste edozein balio gisa).**
6	**DIP/PIDri buruzko testigantza ISO/IEC 18013-5: 2021 arauan zehaztutako datu-ereduaren arabera aurkezteko eman behar da, bai W3Cren v1.1 kredentzial egiaztagarrien datu-ereduarekin.**
7	**DIP/ PIDri buruzko testigantza CBOR gisa eta JSON formatuan kodetu behar da.**
8	**DIP/PIDri buruzko testigantzak atributuen zabalkunde selektiboa ahalbidetu behar du, "Selective Disclosure for JWTs (SD-JWT)" eta "Mobile Security Object (ISO/IEC 18013-5)" eskemaren bidez, datu-ereduaren arabera (Permiso de conducir en el móvil).**
9	**DIP/PIDri buruzko testigantzak sinadura elektronikoak eta zifratzeko formatuak erabili behar ditu, 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-en zehazten den bezala.**
10	**DIP/PIDri buruzko testigantzak sinadura algoritmoak erabili behar ditu, SOG-IS ACM (Agreed Cryptographic Mechanism) arauaren arabera[17].**

3. taula - EIZ emateko baldintzak

5.2. Atributu kualifikatuaren eta kualifikatu gabekoaren testigantza elektronikoa

5.2.1 TE(C) A/(Q) EAAak emateko baldintzak

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

Hurrengo koadroan, testigantza TE(C) A/(Q)EAAei aplikatu beharreko betekizunak zehazten dira, testigantzan jasotako informazioari dagokionez, adibidez, baliozkotasuna, benetakotasuna, baliozkotzea, gakoen kudeaketarekin, datu-ereduarekin eta formatuekin lotutako politikak egiaztatzeko.

TE(C) A/(Q) EAA testigantzak ERE DIP/PID datuei aplikatu beharreko betekizunen arabera eman daitezke.

Testu honen etorkizuneko bertsioek taula handitu ahal izango dute, baldintzak zehazteko. Kontuan izan behar da baldintza horiek IDUE Zorroaren zehaztapenen lehen bertsiora bideratuta daudela, eta zehaztapenak aldatu ahala alda daitezkeela.

#	Betekizuna
1	**TE(C) A/(Q) EAA testigantzek igorlea identifikatzeko behar den informazioa jaso behar dute.**
2	**TE(C) A/(Q) EAA testigantzek datuen osotasuna egiaztatzeko behar den informazioa eman behar dute.**
3	**TE(C) A/(Q) EAA testigantzek benetakotasuna egiaztatzeko behar den informazioa jaso behar dute.**
4	**TE(C) A/(Q) EAA testigantzek beren baliozkotasun-egoera egiaztatzeko behar den informazio guztia jaso behar dute.**
5	**(ez da adierazten)**
6	**TE(C) A/(Q) EAA testigantzek alderdi informatu batek titularraren lotura egiaztatzeko behar den informazio guztia(atributu gisa edo sinatutako beste edozein balio gisa) jaso beharko lukete.**
7	**TE(C)A/(Q)EAA testigantzak datu-ereduaren zehaztapenetako baten arabera eman behar dira: gidabaimenaren kodetze-araua: I"SO/IEC 18013-5:2021", edo W3Cren"Verifiable Credentials Data Model v1.1" (W3Cren 1.1 kredentzial egiaztagarrien datuen eredua).**
8	**TE(C) A/(Q) EAA testigantzak honako formatu hauetako bat bezala kodetu beharko lirateke: CBOR edo JSON, ziurtagirirako erabilitako datu-ereduaren arabera. Ikusi RFC 8812, RFC 8152, RFC 9052, RFC 9053**
9	**TE(C) A/(Q) EAA testigantzak JSON-LD (JSON for Linking Data) bezala kodetu daitezke.**

10	**TE(C)A/(Q)EAA testigantzek atributuen errebelazio selektiboa ahalbidetu beharko lukete, honako hauek erabiliz: "Selective Disclosure for JWTs" (JWTs)(SD-JWT) edo gidabaimenari buruzko arauaren "Mobile Security Object" (Segurtasun Mugikorraren Objektua) eskema(ISO/IEC 18013-5), testigantzarako erabilitako datu-ereduaren arabera.**
11	**TE(C)A/(Q)EAA testigantzek honako sinadura eta zifratu formatu hauetako bat erabili beharko lukete, IETF, RFC(JOSE (Javascript Object Signing and Encryptio) eta COSE (CBOR Object Signing and Encryption) arauetan zehazten denez, testigantzarako erabilitako datu-ereduaren arabera.**
12	**TE(C) A/(Q) EAA testigantzek zifratzeko algoritmoak erabili beharko lituzkete SOG-IS ACM (Agreed Cryptographic Mechanism) arauaren arabera.**
13	**TE(C) A/(Q) EAA testigantzak OpenID4VCI (OpenID for Verifiable Credential Issuance) protokoloaren arabera eman beharko lirateke.**

4. taula - (Q)CEAak emateko baldintzak

6. Erreferentzia-arkitektura eta fluxuak

Erreferentziazko arkitektura IDUE Zorroko soluzioen arkitekturaren diseinu-prozesuan hartutako erabaki-multzo bat da. Hauteskunde horiek IDUE Zorroaren soluzioek hainbat agertoki jasan behar dituzte, non erabiltzailea, konfiantza duen zatia (edo zati informatua) edo biak lineatik kanpo egon behar diren, eta, aldi berean, estatu kideei malgutasuna ematen diete IDUE Zorroaren soluzio bat hainbat osagai-konfiguraziotan ezartzeko.

6.1. Diseinuari buruzko kontsiderazioak

Konplexutasuna mugatzeko, IDUE Zorroaren Soluzioaren hasierako zehaztapenek IDUE Zorroaren instantzia erabiltzailea identifikatzeko erabiltzea ahalbidetzen duten konponbidearen gutxieneko osagai-kopuru bat baino ez dute jasoko, Nortasun Elektronikorako Bitarteko gisa funtziona dezan(eID).

Aukeratutako aukerek ez dute garrantzi erlatiborik islatzen, ezta epe luzerako konpromisorik ere. Horren ordez, hautaketa hainbat faktorek gidatu dute, hala nola arauen eta zehaztapenen erabilgarritasuna eta heldutasuna, adopzio-erraztasunaren estimazioa eta konponbidearen osagai bakoitzak eskaintzen duen malgutasun-maila (baimendutako erabilera-kasuen arabera).

Hemen proposatutako konponbidearen osagaiek agerian uzten dute ISO/IEC 23220 arau-saila erabiltzeko itxaropena, publikoki eskuragarri daudenean, ARF (Cards and security devices for personal identification — Building blocks for identity management via mobile devices) etorkizuneko bertsioetarako.

6.2. Arkitektura-osagaiak

Honako osagai hauek IDUE Zorroaren soluzioa ezartzeko beharrezkoak diren IDUE zorroaren arkitektura eraikitzeko bloke gisa identifikatu dira:

- **Gako kriptografikoak kudeatzeko sistema.** Osagai hori informazio kriptografikoa kudeatzeaz eta biltegiratzeaz arduratzen da, DIP/ PID emisio-prozesuan sortutako gako pribatu gisa, adibidez.

- **Testigantzak trukatzeko protokoloa**. Protokolo honek DIP/PID datuak eta TE(C) A/(Q) EAA testigantzak modu seguruan eta pribatutasuna zainduz nola eskatu eta aurkeztu zehazten ditu. Protokoloak zehazten du, halaber, nola egiten den autentifikazioa Konfiantza duen Alderdiaren (edo Alderdi Informatuaren) eta IDUE Zorroaren Instantziaren artean, bereziki, alderdi informatuak IDUE Karteraren bidez identifikazioa eskatzeko mekanismoa. Eskaerak Alderdi Informatuari eta eskatutako datuei buruzko informazio guztia jasotzen du. Protokolo hori konfiantzaren negoziazioaz eta elkarrekiko autentifikazioaz arduratzen da.

- **Jaulkipen-protokoloa**. Protokoloak DIP/PID eta TE(C) A/(Q) EAA testigantzak nola eman behar diren eta zein formatutan eman behar diren zehazten du.

- **Datu-eredua**. Datu-ereduak datu-elementuak eta beren artean eta horien propietateak nola eragiten dituzten definitzen eta deskribatzen du.

- **DIP/ PID eta TE(C) A/(Q) EAA eskemak**. Lekukotzaren eskemak testigantzaren propietateak eta erabiltzailearen ezaugarriak definitzen dituzten datuen egitura eta antolamendu logikoa jasotzen ditu. Lekukotza-eskemak informazio gehigarria ere jasotzen du, besteak beste, egiaztapen-mekanismoak, azpiko nortasun-bermea (aseguramendu-maila) eta propietateak zerrendatzeko konfiantza-esparrua, bai eta erabiltzaile legitimoaren edukitza-proba ere.

- **DIP/ PID eta TE(C) A/(Q) EAA formatuak**. DIP/PID eta TE(C) A/(Q) EAA formatuak pertsona fisiko edo juridiko baten edo objektu baten ezaugarria, ezaugarria, eskubidea edo baimena adierazteko erabiltzen dira, elektronikoki sinatutako eta egiazta daitezkeen lehergailu digital gisa, interoperabilitaterako edozein jabetza gehigarri dutenak.

- **Sinadura-formatuak**. Artefaktu digital gisa metodo matematiko baten edo batzuen inplementazio teknikoa, dokumentu digital baten benetakotasuna, osotasuna, dokumentu baten egilea kautotzeko eta, aukeran, hartzailea (dokumentuaren entzunaldia) frogatzeko.

- **Konfiantza-eredua.** IDUE Zorroaren azpiegituran esku hartzen duten osagaien eta erakundeen zilegitasuna bermatzen duten arauen multzoa, hauek barne hartzen dituztenak:
  - Erabiltzaileen autentifikazioa.
  - Jaulkitzailearen identifikazioa.
  - Jaulkitzaileen erregistroa.
  - Datu-ereduak eta aitortutako eskemak.
  - Alderdi Informatuen erregistroa eta autentifikazioa.
  - Konfiantza ezartzeko mekanismoak, multidominio anitzeko eszenatoki batean.

  Konfiantza-ereduaren osagaiek IDUE Zorroan konfiantza duten erakundeak identifikatzeko aukera ematen dute, eta funtsezkoak dira informazioaren benetakotasunerako, konfidentzialtasunerako, osotasunerako eta baimen informaturako(sinadura elektronikoetan eta zigiluetan). Konfiantza-eredu desberdinak daude, hainbat arautan oinarrituak.

Konfiantza-zerrenda mekanismo bat da, konfiantza-eredu baten esparruan, agintaritza duten zatiei buruzko informazioa argitaratzeko eta lortzeko, adibidez, DIP/PID, TE(C) A/(Q)EAA testigantzak eta informatutako zatiak.

- **Suiteak eta mekanismo kriptografikoak**. Datu-trukea konfidentzialtasunari eta osotasunari dagokienez ziurtatzen duten algoritmoak eta metodoak.

- **Erakundearen identifikatzaileak**. Datu-ereduko elementu guztietarako identifikatzaile bakarrak.

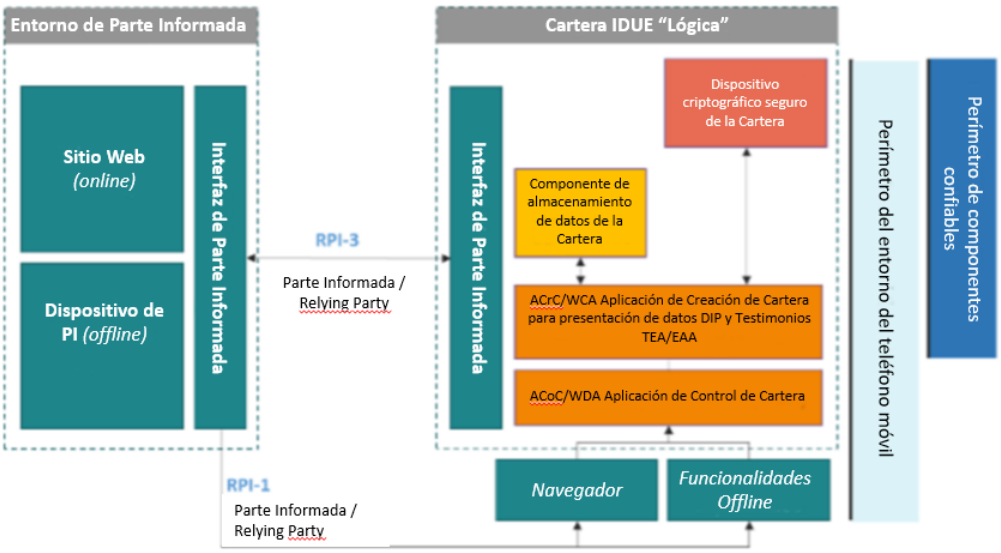
- **Baliozkotasun-egoera egiaztatzea**. Besteak beste, DIP/PID datuen, TE(C) A/(Q) EAA testigantzen, sinadurak edo zigilu elektronikoak egiteko ziurtagirien eta abarren baliozkotasun-egoerari buruzko informazioa argitaratzeko eta lortzeko mekanismoa.

6.3. Arkitektura logikoa

IDUE Karterako soluzio batek gailu mugikor batean gauzatzen den aplikazio bat duenean, aplikazio horren parte ez diren baina, hala ere, IDUE Zorroaren baliabide logikoen parte diren konfiantzazko osagai gehigarrien beharra egon daiteke. Behar hori hainbat arrazoirengatik sor daiteke:

- Segurtasuna: adibidez, gailu jakin batek hardware segururik ez badu, hala nola,"Secure Element" (elementu segurua, sakelako telefono askoren ekipamendu estandarra), kanpoko hardware-osagaiak beharrezkoak izan daitezke, hala nola txartel adimendunak.
- Sistemak urrutiko zerbitzari-inguruneetan berrerabiltzea (backend).
- Erabiltzailearengan zentratutako nortasun-azpiegitura berrerabiltzea (batzuetan nortasun deszentralizatua).

Konfiantza-osagai horiek honako hauek izan daitezke: konfiantzazko kanpo-biltegiratzea, kanpoko hardware integratua edo konfiantzazko hardware integratua edo IDUEs Zorroko urruneko beste osagai batzuk. Jarraian, IDUE Zorroko osagaien ezarpenean izandako aldaketen irudikapen kontzeptuala erakusten da:



ACrA/WCA: Sortu DIPren eta Alderdi Informatuarekin partekatzen diren Testigantza Kualifikatuen aurkezpena(egiaztagarria) , ACC/WDAtik jasotako informazioaren arabera.

ACoC/ WDA: Erabiltzaileak aukeratutako datuak ematen ditu:

- DIP eta testigantzak (konbina daitezke)
- Zehaztu zein (edo ez) aurkez daitezkeen

6 irudia: IDUE Zorroaren konfigurazioen kontzeptu-eredua

Hurrengo taulak IDUE zorroaren osagaiak 6 irudiaren kontzeptu-ereduarekin erlazionatzen ditu.

Bloke funtzionala kontzeptu-ereduan	IDUE Karterako konponbideari aplikatu beharreko osagaiak
IDUE Zorroaren gailu kriptografiko segurua	Erabiltzaile-gakoak eta ziurtagiriak
	Ingurune segurua eta isolatua gako eta datuetarako
	Algoritmo kriptografikoak (adibidez, simetrikoak, asimetrikoak, gakoen deribazioa, hash funtzioak, zenbaki aleatorioen sorrera) eta protokoloak (adibidez, ECDH, TLS).
	Gako eta datuetarako hardwqrek definitutako ingurune segurua: elementu segurua (SE), Konfiantza Gauzatzeko Inguruneak (Trusted Execution Environment -TEEs), Hardware -ko Segurtasun Modulua (Hardware Security Module - HSM), etab. (remotoa edo lokala).
	Autentifikazio datuak (PIN, biometria)
IDUE zorroko datuak biltegiratzeko osagaiak	Erabiltzailearen identifikatzaile bakarra eta iraunkorra
	Erabiltzailearen atributuak
	Erabiltzailearen datu pertsonalak eta atributuak
	Gako eta datuentzako ingurune segurua

IDUE kartera"DIP/PID edo TEA/ EAAren aurkezpena" Kartera sortzeko aplikazioa (WCA - Wallet Creation Application)	Erregistroak, Eskabideko eragiketen historiala IDUE kartera, telemetria
	IDUE Kartera aplikazio-orriaren identifikatzailea (adibidez, konfigurazioa, fabrikatzailea eta bertsioa)
	IDUE Karterako instantziaren barne-interfazeak (adibidez, biltegiratzea, osagaiak, zifratua)
IDUE Zorroaren kontrolaren aplikazioa (WDA, Wallet Driving Application)	Erregistroak, Eskabideko eragiketen historiala IDUE kartera, telemetria
	IDUE KarteraKo Eskaeraren aplikazioaren identifikatzailea (adibidez, konfigurazioa, fabrikatzailea eta bertsioa)
	IDUE Zorroaren erabiltzaile-interfazea
Informatutako zatiaren interfazea	IDUE Zorroaren interfazea (Q)TSP, TE(C) A/(Q)EAA hornitzaileekin, estatu kideetako azpiegiturekin, e-IDa nazionalekin, konfiantza duten zatiekin eta EEAko beste iturri batzuekin.
	IDUE zorroaren eta beste alde batzuen arteko komunikazio-kanalak(lineatik kanpo)

5. taula - IDUE zorroko osagaien eta kontzeptu-ereduaren bloke funtzionalen arteko lotura

Hurrengo taulak IDUE Karterako osagaiak 6 irudian ordezkatutako bi perimetroei esleitzen dizkie.

Perimetroak	**IDUE Kartera soluzioari aplikatu beharreko osagaiak**
Konfiantzazko osagai posibleen perimetroak	Gailuari buruzko informazioa (mota, konfigurazioa, firmware bertsioa, egoera, etab.)
	Sistemaren gakoak eta ziurtagiriak
	Back-end sistemak (datu-baseen zerbitzariak)
	Konfiantzazko gailu konektatuak
Perimetro mugikorr potentziala	Gailuari buruzko informazioa (mota, konfigurazioa, firmware bertsioa, egoera, etab.)
	Smartphone-aren sentsoreak: kamera, NFC irakurlea, hatz-marken sentsorea, azelerometroa, etab.

6. taula: IDUE zorroaren osagaien eta perimetroen arteko korrespondentzia

6.4. Fluxu motak

Atal honek IDUE Kartera horrek maila orokorrean jasan behar dituen lau fluxu-motak deskribatzen ditu. Lau fluxuak honako hauek dira:

1. Hurbiltasun-fluxu gainbegiratua.
2. Gainbegiratu gabeko hurbiltasun-fluxua.
3. Gailuen arteko urruneko fluxua.
4. Gailu beraren urruneko fluxua.

1 eta 2 fluxuak IDUE Zorroaren erabiltzailea fisikoki fidatzen den zati batetik gertu dagoen egoera batekin lotuta daude (parte informatua) eta lekukotzen trukea eta zabalkundea (DIP/PID eta/edo TECA/QEAA) hurbiltasun-protokoloak erabiliz egin behar dira (NFC, Bluetooth, QR-Code, etab.), eta erabiltzaileak ez du Interneterako konektibitaterik (ez da esan nahi garraioaz aparte beste edozein funtzio posible denik). konexiorik gabe). Hurbiltasuneko bi fluxuak alde batetik bestera daude. Gainbegiratutako fluxuan, IDUE Karterako atributu egiaztagarriak ditu, edo, gainbegiratuta, alderdi informatu gisa jarduten duen pertsona bati (dispositibo propio batek jardun dezakeena). Gainbegiratu gabeko fluxuan, IDUE Karterako atributu egiaztagarriak ditu giza ikuskaritzarik gabeko makina bati.

3 eta 4 fluxuak Internet bidez datu-trukea egin behar den eszenatoki batekin lotuta daude. Urrutiko bi fluxuak alde batetik bestera daude. Gailuen arteko urruneko fluxuan, IDUE Zorroaren erabiltzaileak zerbitzuari buruzko informazioa kontsumitzen du IDUE Zorroaren gailua ez den beste gailu batean, eta saioa ziurtatzeko bakarrik erabiltzen da (adibidez, IDUE Kartera erabiliz QR kode bat eskaneatzeko saio hasierako orrialde batean, bere web nabigatzailean banku-kontu bat sartzeko). Aldiz, gailu beraren urruneko fluxuan, IDUE Zorroaren erabiltzaileak IDUE Zorroaren gailua erabiltzen du, bai saioa ziurtatzeko, bai zerbitzuaren informazioa kontsumitzeko.

Erabiltzaileen esperientziak deskribatutako lau fluxuetako batean oinarrituko dira, gutxienez, eta, ziurrenik, horien konbinazio batean. Ikus bedi lau fluxuak era askotara inplementa daitezkeela. Berariazko inplementazioak testu honen eremutik kanpo geratzen dira.

Hurbiltasuneko bi fluxuak aztertzen jarraitu behar da, Interneterako konexioarekin edo konexiorik gabe posible baitira. Agertoki posibleen artean honako hauek daude:

- Erabiltzailea eta Alderdi Informatua linean daude biak,
- erabiltzailea bakarrik konektatuta,
- Alderdi Informatua bakarrik lerroan,
- Erabiltzailea eta Alderdi Informatua deskonektatuta daude.

Aurretik deskribatutako fluxu guztietarako eta, zehazki, hurbiltasun-fluxu gainbegiratu gaberako, erabiltzailearen baimena datuak trukatzeko aldez aurreko baldintza da.

Jarraian, DIP/PID eta TEA/EAA (etorkizunean konfigurazioak gehitu ahal izango dira, beharrezkoa den moduan) zehazten dira.

6.5. Zorroaren konfigurazioak

6.5.1. Justifikazioa

IDUE Kartera garatzearen helburuetako bat DIP/PID datuak eta TE(C) A/(Q) EAA testigantzak mugan zehar harmonizatzea da. Horrek, era berean, konplexutasuna mugatzeko konponbide tekniko oso txikia eskatzen du, eta horrek ezarpena eta adopzioa errazten ditu. Bestalde, IDUE Zorroaren zehaztapenak hainbat baldintza betetzen dituen erabilera-kasu ugariri euskarria eman behar die. Desberdintasun horiek DIP/PID datuak eta TE(C) A/(Q) EAA testigantzak sortzeko, eskatzeko eta aurkezteko modu espezifikoak eragiten dituzte. Behar horiek asetzeko, IDUE Zorroko soluzioek konfigurazioak ezarriko dituzte. Konfigurazio bat IDUE Karterako Konponbidearen gaitasun teknikoak erabiltzeko murrizketa eta moduen multzo espezifikoa da, DIP/PID multzoa eta TE(C) A/(Q) EAA testigantzak kudeatzeko.

Konfigurazio baten lehen helburua IDUE Karterako gaitasun espezifikoak gaitasun horiekin bete daitezkeen erabilera-kasuen betekizunekin lotzea da. Konfigurazio bakar batek erabilera-kasu ugari jasan behar ditu; bakoitza DIP/PID edo TE(C) A/(Q) EAA testigantza emateko berariazko konfigurazioaren arabera.

Konfigurazio baten bigarren eta azken helburua ingurune teknologikoak eta IDUE Karterako Soluzioaren zehaztapenen ezaugarriak potentzialki handitzeko tresna bat ematea da. Erabilera-kasu bat edo erabilera-kasu talde bat ezin bada oinarritu IDUE Zorroaren Soluzioaren lehengo konfigurazioan, konfigurazio gehigarri bat sartu behar da, dauden konfigurazioekin bete ezin diren betekizunei euskarria emateko. 8. kapituluan gobernantza eta konfigurazio berriak gehitzeko prozesua deskribatzen dira.

6.5.2. Hasierako konfigurazioak

IDUE Zorroaren soluzioek bi konfigurazio onartuko dituzte hasiera batean:

- 1. motako **konfigurazioa** berariaz zuzenduta, baldin eta informatutako alderdiak nortasunaren goi-mailako aseguratze-mailarako eskatzen diren bermeetan konfiantza badu(LoA High), CIR 2015/1502 Betearazpen Erregelamenduan definitzen den bezala[18] , mugaz gaindiko identifikazioa ahalbidetzeko, DIP/PID atributuak erabiliz nortasuna segurtatzeko mailan (LoA High). 1 motako konfigurazioa DIP/ PID nortasun-datuak ezartzeko diseinatuta nagusiki.
- 2 motako **konfigurazioaren** helburua da malgutasuna eta ezaugarri gehigarriak izatea, 1 motako konfigurazioarekin ase ezin diren TE(C) A/(Q) EAA testigantzak erabili ahal izateko.

[18] Batzordearen 2015eko irailaren 8ko 2015/1502(EB) Betearazpen Erregelamendua, identifikazio elektronikoko bitartekoen berme-mailei buruzko gutxieneko zehaztapen teknikoak eta prozedurak ezartzen dituena, Europako Parlamentuaren eta Kontseiluaren 910/2014(EB) Erregelamenduaren 8.3 artikuluaren arabera, barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantza-zerbitzuei buruzkoa.

Kontuan izan behar da 1 motako konfigurazioa ez dagoela DIP/ PID multzorako bakarrik pentsatuta. Litekeena da te(C) A/(Q) EAA testigantza asko aseguru-maila altuak behar dituzten eremuetan erabiltzea (adibidez, finantzak, osasuna, eraikinetarako sarbidea) eta 1 motako konfigurazioarekin betetzen diren baldintzak izatea. Hala izanez gero, TE(C) A/(Q) EAA horiek 1 motako konfigurazioaren arabera emango dira.

6.5.3. Konfigurazio-betekizunak

Atal honek konfigurazioen baldintzak ezartzen ditu, 1 motako eta 2 motako konfigurazioa hainbat baldintza-taldetan alderatuz. Testu honen etorkizuneko bertsioek taula handitu ahal izango dute, jaulkitzaileei eta konfiantza duten alderdiei buruzko betekizunak zehazteko. Kontuan izan behar da baldintza horiek IDUE Zorroaren Soluzioaren zehaztapenen lehen bertsiora bideratuta daudela batez ere, eta zehaztapenak aldatu ahala alda daitezkeela.

Hurrengo taulak IDUE Zorroaren Soluzioaren osagaiei bi konfigurazioak jasateko aplikatu beharreko baldintzak zehazten ditu. Konfigurazio motaren arabera, baldintza horrek esan nahi du puntu suspentsiboak [...] ordeztu behar direla 1 edo Tipo 2 (DEBE, DEBERÍA, etab.) zutabean adierazitako aditzarekin.

Osagaia	**Betekizuna**	**1. mota**	**2. mota**
Gako kriptografikoak kudeatzeko sistema - 1	IDUE [...] Kartera konpontzea, gako kriptografikoak biltegiratzeko eta kudeatzeko osagai hauetako batean oinarritu behar da: Elementu segurua (SE) integratua edo gailu mugikorretarako ingurunea, kanpoko gailu baten mendekotasuna (elementu seguruak / txartel adimendunak), eta zerbitzari bat (urruneko hardwarearen segurtasun-modulua). hardware segurua aukeratzea IDUE Zorroaren soluzio bakoitzaren arabera erabiliko da eta jasango da.	ZOR	BEHARKO LUKE
Gako kriptografikoak kudeatzeko sistema - 2	IDUE [...] Zorroaren soluzioak segurtasun-neurriak aplikatzea sekretu kriptografikoen esportazioa saihesteko.	ZOR	BEHARKO LUKE

Testigantzak trukatzeko protokoloa - 1	IDUE [...] Karterako soluzioa OpenID4VP jasan behar da, urruneko fluxuetarako testigantzak trukatzeko protokolo gisa **.** Autentifikazio pseudonimoa eskatzen denean, eskabide-parametroak OpenID SIOPv2 zehaztapenaren arabera zehaztu beharko lirateke.	ZOR	BALITEKE
Testigantzak trukatzeko protokoloa - 2	ISO/IEC 18013-5: 2021 arauan zehaztutako protokoloa **, hurbiltasun fluxuetarako**.	ZOR	BALITEKE
Testigantzak trukatzeko protokoloa - 3	IDUE [...] Kartera konpontzea, bilkuraren lotura betetzeko egiaztapenak egitea (hau da, DIP/PIDrako atributu-eskaera).	BEHARKO LUKE	BALITEKE
Testigantzak trukatzeko protokoloa - 4	IDUE [...] Karterako soluzioa testigantzak trukatzeko protokolo-aukerak jasan behar dira[19].	BALITEKE	BALITEKE
Testigantzak trukatzeko protokoloa - 5	IDUE [...] Kartera-zorroaren soluzioa edukitza-proba bat egin ahal izatea.	ZOR	BALITEKE
Testigantzak trukatzeko protokoloa - 6	IDUE [...] Kartera konpontzea, ISO/IEC 18013-5: 2021 arauan zehazten den bezala.	ZOR	BALITEKE
Testigantzak trukatzeko protokoloa - 7	IDUE [...] Kartera-zorroaren soluzioak atributuen dibulgazio selektiboa jasan behar du, SD-JWT zehaztapenean zehazten den bezala.	ZOR	BALITEKE
Emisio-protokoloa - 1**	IDUE [...] Kartera-konponbidea OpenID4VCI onartzea emisio-protokolo gisa. Estatu kideek libre dira beren konponbide nazionaletan emisio-protokoloaren alternatiba gehigarriak sartzeko.	DEBE **	ZOR

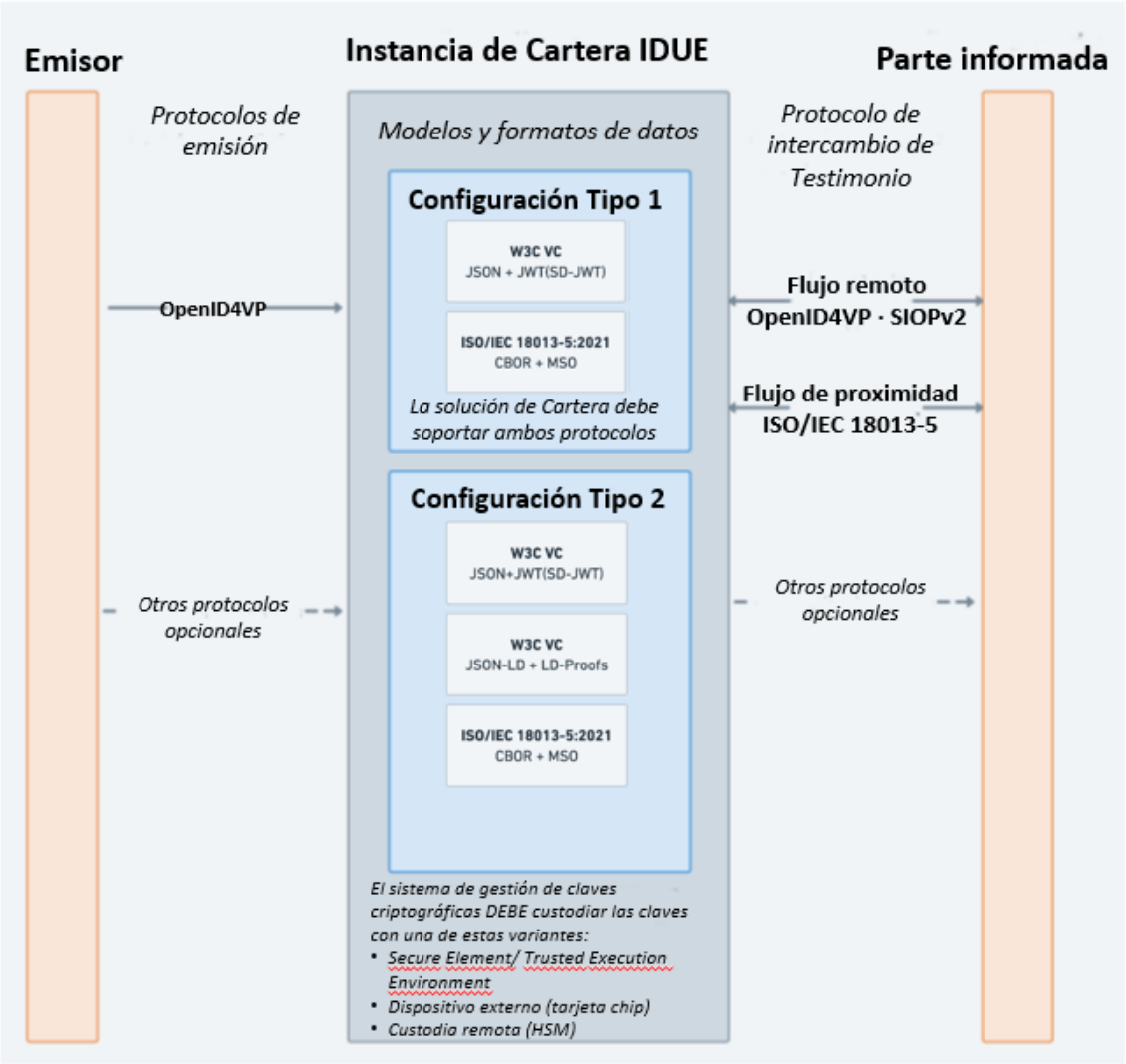
[19] Aipatzekoa da Mdoc-en API REST,ISO/ IEC 23220-4 zirriborroan zehazten den bezala.

Datu-eredua -1	IDUE [...] Kartera konpontzea iSO/IEC 18013-5: 2021 arauan zehaztutako datu-ereduaren arabera emandako testigantzak onartzea.	ZOR	BEHARKO LUKE
Datu-eredua -2	IDUE [...] Karterako soluzioak W3C Verifiable Credentials Data Model 1.1 zehaztapenean zehaztutako datu-ereduaren arabera emandako testigantzak jasan behar ditu.	ZOR	BEHARKO LUKE
DIP/PID eta TE(C) A/(Q) EAA - 1 formatuak	IDUE [...] Karterako soluzioa JWT eta SD-JWT formatuko testigantzak jasan behar dira.	ZOR	BALITEKE
DIP/PID eta TE(C) A/(Q) EAA - 2 formatuak	IDUE [...] Karterako soluzioa CBOR formatuan onartzea.	ZOR	BALITEKE
DIP/PID eta TE(C) A/(Q) EAA - 3 formatuak	IDUE [...] Karterako soluzioa JSON-LD formatuan.	BALITEKE	BALITEKE
Sinadura formatuak -1	IDUE [...] Karterako soluzioak sinadura elektronikoko eta zifratzeko formatuak jasan behar ditu, JOSE (JWT) zehaztapenen arabera.	ZOR	BALITEKE
Sinadura formatuak - 2	IDUE [...] Kartera konpontzeak sinadura eta zifratze formatuak jasan behar ditu, COSE zehaztapenen arabera.	ZOR	BALITEKE
Sinadura formatuak - 3	IDUE [...] Kartera konpontzeak sinadura eta zifratze formatuak onartzea, LD-Proof zehaztapenen arabera.	EZ ZOR	BALITEKE
Suiteak eta mekanismoak kriptografikoak - 1	IDUE [...] Zorroaren Soluzioa SOG-IS Agreed Cryptographic Mechanisms Version 1.2-n zehaztutako atributuetarako erabiltzen diren suite kriptografikoak eta mekanismoak jasan behar dira.	ZOR	BEHARKO LUKE

7. taula - Konfigurazio-baldintzak

*** Interoperabilitatea bermatzeko emisio-protokolo komuna izan behar duten TE(C) A/(Q) EAA testigantzetarako bakarrik. DIP/PID datuen kasuan, estatu kideari dagokio emisio-protokoloa zehaztea, eta zorro-soluzio bakoitzak berariazko DIP/PID isurtze-protokoloa izango du, estatu kidearen zehaztapenen arabera.*

IDUE Karterako soluzioek **1 motako** konfigurazioa jasan **behar** dute, DIP/ PIDrako derrigorrezkoa dena.



7. irudia. IDUE Karterako konfigurazioak.

7. IDUE zorroen ziurtapen-prozesua

Estatu kideek, EIDen Erregelamendua erreformatzeko proposamenaren 6 quater (3) artikuluarekin bat etorriz, egokitasuna ebaluatzeko erakunde egiaztatuak izendatu behar dituzte, IDUE zorroen egokitasunaren ebaluazioa gainbegiratzen dutenak. Izendapen-prozesu hori estatu kideen artean bateratu behar da.

Izendapen hori egin ondoren, estatu kideek Europako Batzordeari jakinaraziko dizkiote erakunde publiko edo pribatu horien izenak eta helbideak, proposamen horren 6 quater artikuluaren 5 paragrafoaren arabera.
IDUE zorroaren hornitzaileak izendatutako OEC/CAB bati edo batzuei eskatu behar die(hautaketatu, kontratatu) IDUE zorroa EIDAS Erregelamenduaren betekizunekin bat datozen ebaluatzen eta egiaztatzen dutenei.

IDUE Karteraren ziurtagiria OEC/CAB-k egiten du, IDUE (ziurtagiriaren helburua) kartera zehaztapen tekniko eta operatiboei eta erreferentzia-arauei buruz ezarritako betearazpen-egintzetatik eratoriko arau-agiriekin bat datorren ebaluazioa eta ziurtatzeko.

IDUE Kartera ziurtatuta egon beharko da adostasun-ebaluazioak bermatzeko, baina baita segurtasun-maila handiak betetzen direla frogatzeko ere. Zibersegurtasuna ziurtatzeko sistema bat erabiltzeak IDUE Zorroaren segurtasunean konfiantza-maila bateratua ekarri beharko luke. Material kriptografikoaren biltegiratze segurua zibersegurtasun ziurtagiriaren mende egotea espero da.

IDUE zorro-hornitzaileen ziurtapen-prozesuak Zibersegurtasunari buruzko Erregelamenduan edo horien zatietan dauden ziurtapen-sistema egokiak eta batzuk erabiltzeko aprobetxatu, oinarritu eta eskatu behar [20] du, zorroak edo horien zatiak zibersegurtasun-betekizun aplikagarriekin bat datorren egiaztatzeko.

[20] 2019/881(EB) ERREGELAMENDUA, EUROPAKO PARLAMENTUARENA ETA KONTSEILUARENA, 2019ko apirilaren 17koa, ENISA (Zibersegurtasunerako Europar Batasunaren Agentzia) eta informazioaren eta komunikazioaren teknologien zibersegurtasunaren ziurtapenari buruzkoa eta 526/2013(«Zibersegurtasunari buruzko Erregelamendua») Erregelamendua indargabetzen duena)

8. Arkitekturaren eta erreferentzia-esparruaren garapen-prozesua

8.1. Argitalpena

Dokumentu hori eta egiteke dauden elementuak jendearen eskura jartzen dira https://code.europa.eu/eudi/architecture-and-reference-framework helbide elektronikoan, eta aldian-aldian eguneratuko da, 8.2 kapituluan deskribatutako lan-fluxuaren arabera.

8.2. Eguneratzea

Dokumentu hau egiteko eta eguneratzeko etengabeko aurrerapen azkarra bermatzeko, hurrengo lan-prozesu eta-metodologia aplikatzen da.

EIDAS (E03032) Adituen Taldeak[21] backlog bat izan beharko du, eta lan-elementuen zerrenda lehenetsia da, IFK osatzeko. Egiteke dauden zereginen zerrenda eguneratuko da eIDAS Adituen Taldearen, HaDEA Agentziak(DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID) bultzatutako Eskala Handiko Proiektu [22]Pilotuen, Batzordearen edo interesa duten beste alderdi batzuen iruzkinen arabera, hala nola normalizaziorako nazioarteko erakundeak. Adibidez, IDUE (Framework Contract for Fixed Price and Quoted Time and Means for Development, Consultancy and Support for the European Digital Identity Wallet) karterako erreferentzia-inplementazioaren garapenaren emaitzek[23] eta zehaztapen teknikoen zirriborroek lan-elementu berriak eragin ditzakete.

Europako Batzordeak (DG CONNECT) atzeratutako gaiei buruzko lana antolatuko du, eta lanak aurreikusitako egutegiaren arabera aurrera egin ahal izango du.

EIDen Aditu Taldeak, aldian behin, IFK eguneratzeko, egoki den gai bakoitzarekin zerikusia duten konponbide teknikoei, gomendioei eta betekizunei buruzko hainbat proposamen eztabaidatu eta alderatuko ditu. Horri dagokionez, EIDAS Adituen Taldeak Arkitekturako Erabakien Erregistroen zerrenda bat izango du (RDA, ingelesez ADR, Architecture Decission Records), arFen deskribatutako erabaki teknikoen jarraipena egin eta ulertu ahal izateko.

Dokumentu honen edozein aldaketa eta/edo eguneratze eIDAS Aditu Taldeak adostu beharko du. Adituen taldea aldian behin bilduko da dokumentu horren bertsio berriak eztabaidatu eta onartzeko, bai eta oraindik garatu gabe dauden lanak eguneratzeko ere.

[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

Dokumentu hori Nortasun Digitalaren Europako Esparruaren proposamenaren lege-negoziazioen emaitzara egokituko da, eta, ondorioz, eguneratu egingo da.

8.2.1. Dokumentuen bertsioak

Interoperabilitate-arazoak saihesteko eta IFKn aldaketak oharkabean pasa ez daitezen, IFKrentzat bertsioak kontrolatzeko sistema bat eta bertsioen hurrengo eskema semantikoa erabiliko dira.

ARF dokumentuak bertsio zenbaki jakin bat izango du formatuari jarraituz *NAGUSIA. TXIKIAGOA. PARTXEA*, non:

MAYOR **bertsioa handitu egiten da (hau da, bertsio berri bat), ARF dokumentuak aldaketa esanguratsuak jasan dituenean, adibidez, arkitekturan aldaketa erradikal batzuk sartuz,**

Bertsio **txikia** handitu egiten da dokumentuari informazio berria gehitu zaionean edo dokumentuaren informazioa ezabatu denean, eta

PARCHE bertsioa handitu egiten da aldaketa txikiak egin direnean (adibidez, erraten zuzenketa).

9. Erreferentziak

[IFKn exijentzia-mailak adierazteko gakoak] 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. eta D. Chadwick, "Verifiable Credentials Data Model 1.0", 2019ko azaroaren 19a, <https://www.w3.org/TR/vc-data-model>.

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

[OpenID4VCI] Lodderstedt, T., Yasuda, K., eta T. Looker, "OpenID for Verifiable Credential Issuance", 2022ko abenduaren 30a, https://openid.net/specs/openid-4verifiable-kredential-issuance.html

[SIOPv2] K. Yasuda, T. Lodderstedt, M. Jones, "Self-Issued OpenID Provider V2", 2023ko urtarrilaren 1a, 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

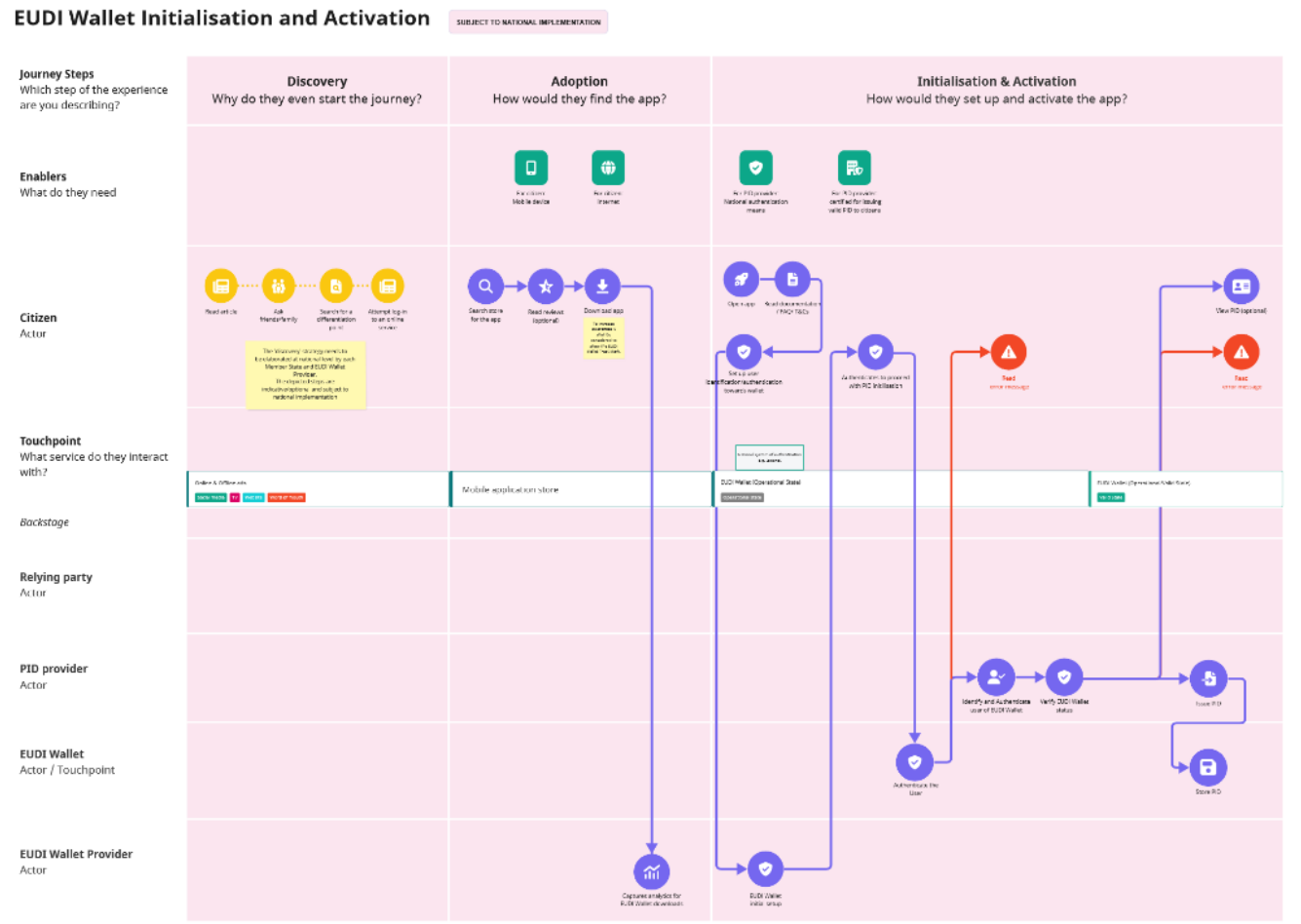
[JOSE] RFC7515 https://www.rfc-editor.org/rfc/rfc7515.html,
https://www.rfc-editor.org/rfc/rfc7516.html RFC7516,
https://www.rfc-editor.org/rfc/rfc7517.html RFC7517,
editor.org/rfc/rfc7518.html-RFC7518 https://www.rfc

[SOG-IS] Adostutako mekanismo kriptografikoak 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/

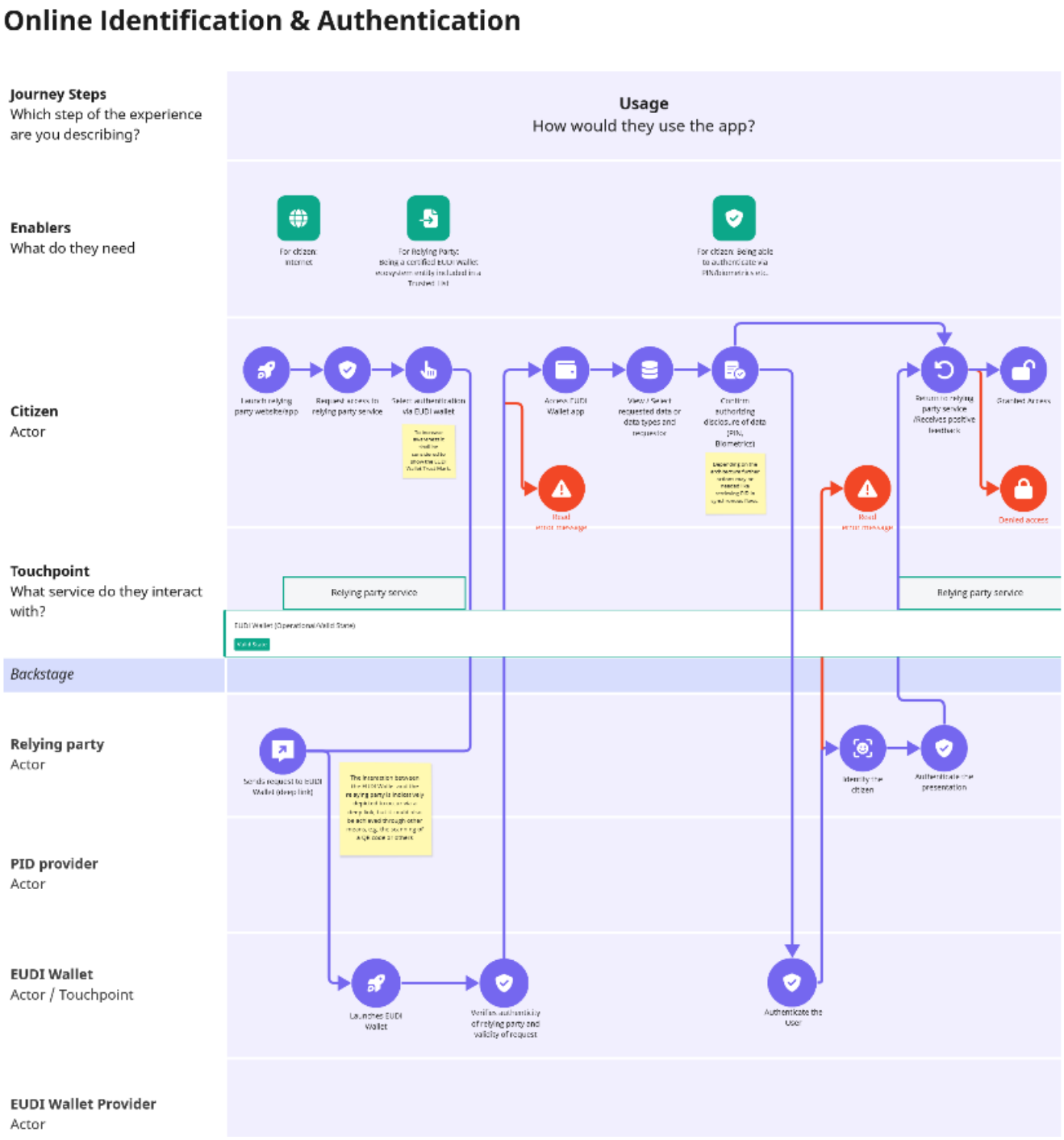
01 Eranskina - inizializazioa eta aktibazioa

Zorroaren inizializazioari eta aktibazioari buruzko zerbitzu-eredua 01 eranskineko artxiboan azaltzen da ***- EUDI Wallet - Initialisation and Activation.pdf***



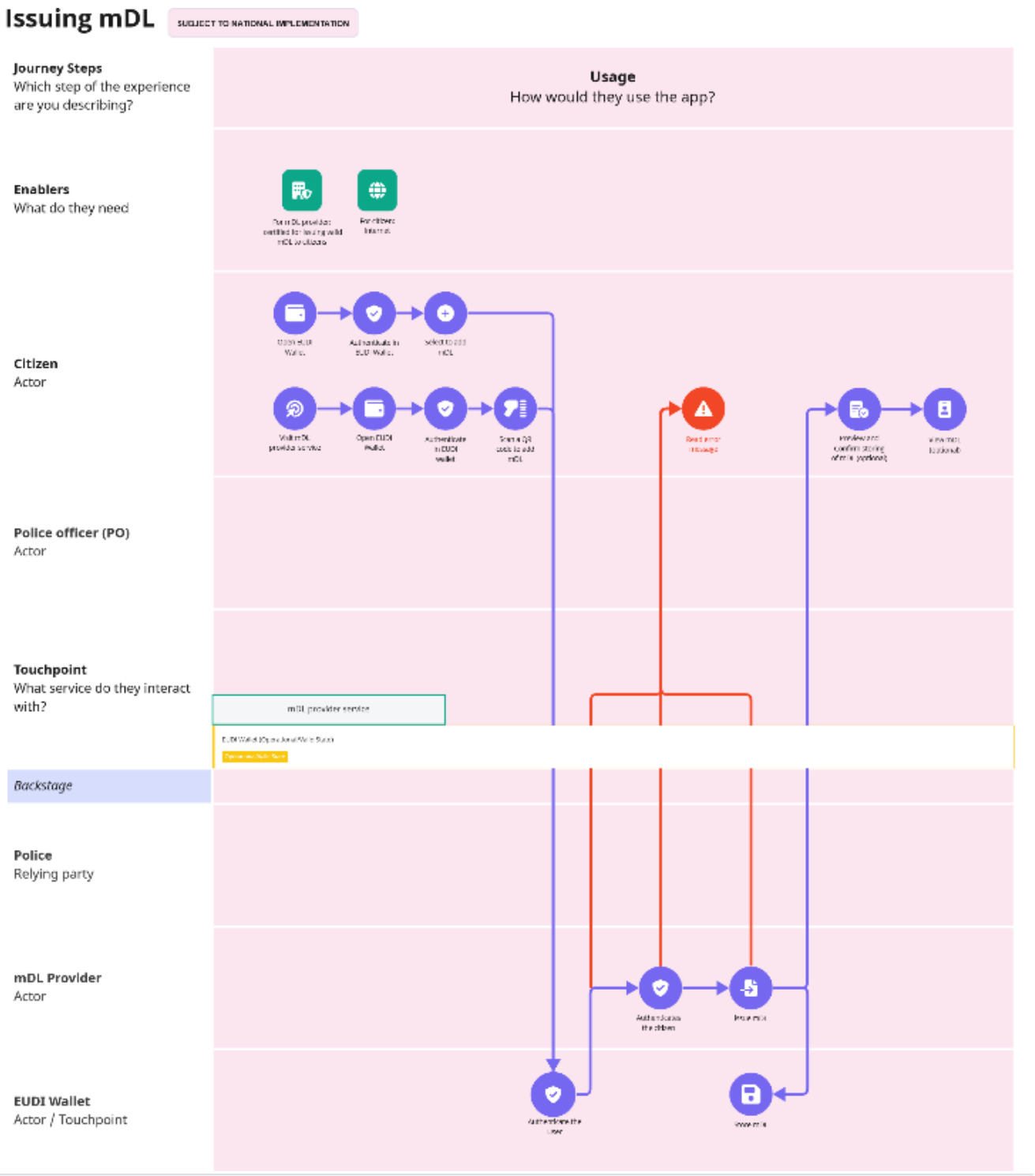
02 Eranskina - lineako identifikazioa eta autentifikazioa

Zorroaren identifikazioari eta lineako autentifikazioari buruzko zerbitzu-eredua 02 eranskineko artxiboan- ***EUDI Wallet - Online Identification and Authentication.pdf***



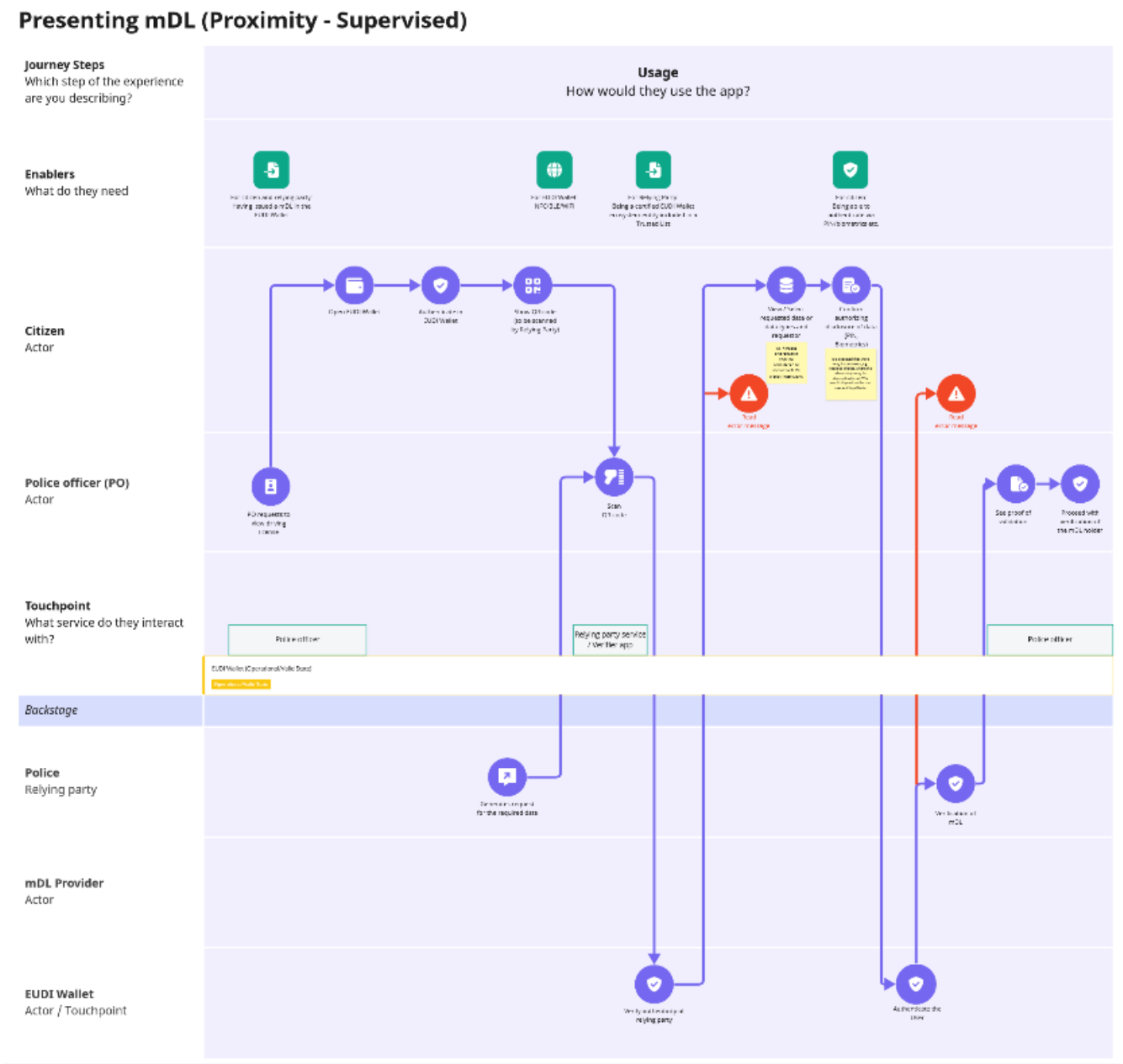
03 Eranskina - MDL ematea

MDL emisioari buruzko zerbitzu-proiektua ***03 - EUDI Wallet - issuing mDL.pdf artxibo erantsian deskribatzen da***.



04 Eranskina - mDLren aurkezpena (proximitysupervised)

MDL (gainbegiratuta) ***aurkezpenari buruzko zerbitzu-proiektua*** 04 - EUDI Wallet - presenting mDL (proximity-supervised) .pdf ***artxibo erantsian deskribatzen da***.



05 Eranskina - mDLren aurkezpena (proximityunsupervised)

mDL (hurbiltasuna-gainbegiraketarik gabe***) aurkezteari buruzko zerbitzu-proiektua*** 05 - EUDI Wallet - presenting mDL (proximity-unsupervised) .pdf ***artxibo erantsian deskribatzen da***.