Amit jelenleg tudunk az eIDAS szerinti wallet-ről...

Szabó Áron

2023-06-30

Nevezd meg! - Így add tovább! 4.0 Nemzetközi (CC BY-SA 4.0)

A jogszabálytervezet szerint mi a wallet?

'European Digital Identity Wallet' is an electronic identification means that allows the user to store identity data, electronic attestations of attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals;

EWC - EU Digital Identity Wallet Consortium (magyar partner van)
- https://eudiwalletconsortium.org/

DC4EU - Digital Credentials 4 European Union (magyar partner van)
- https://www.dc4eu.eu/

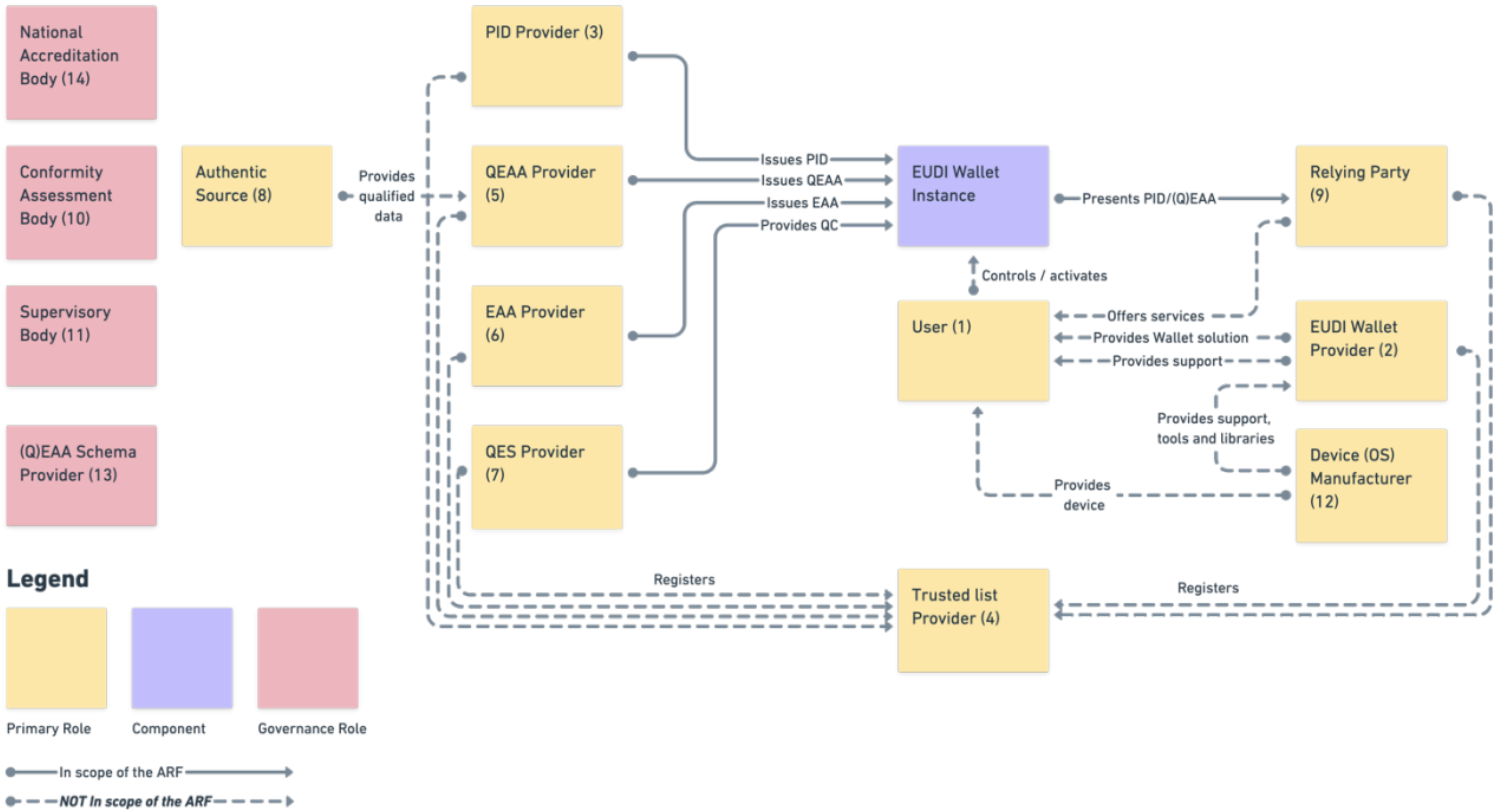
POTENTIAL - PilOTs for EuropeaN digiTal Identity wALlet (magyar partner van)
- https://www.digital-identity-wallet.eu/

NOBID - Nordic-Baltic eID (magyar partner nincs)
- https://www.nobidconsortium.com/

MELASZ

A jogszabálytervezet szerint mi a wallet?

'European Digital Identity Wallet' is an electronic identification means that allows the user to store identity data, electronic attestations of attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals;



eIDAS 2.0 – EUDI wallet

MELASZ

A jogszabálytervezet szerint mi a wallet?

'European Digital Identity Wallet' is an electronic identification means that allows the user to store identity data, electronic attestations of attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals;

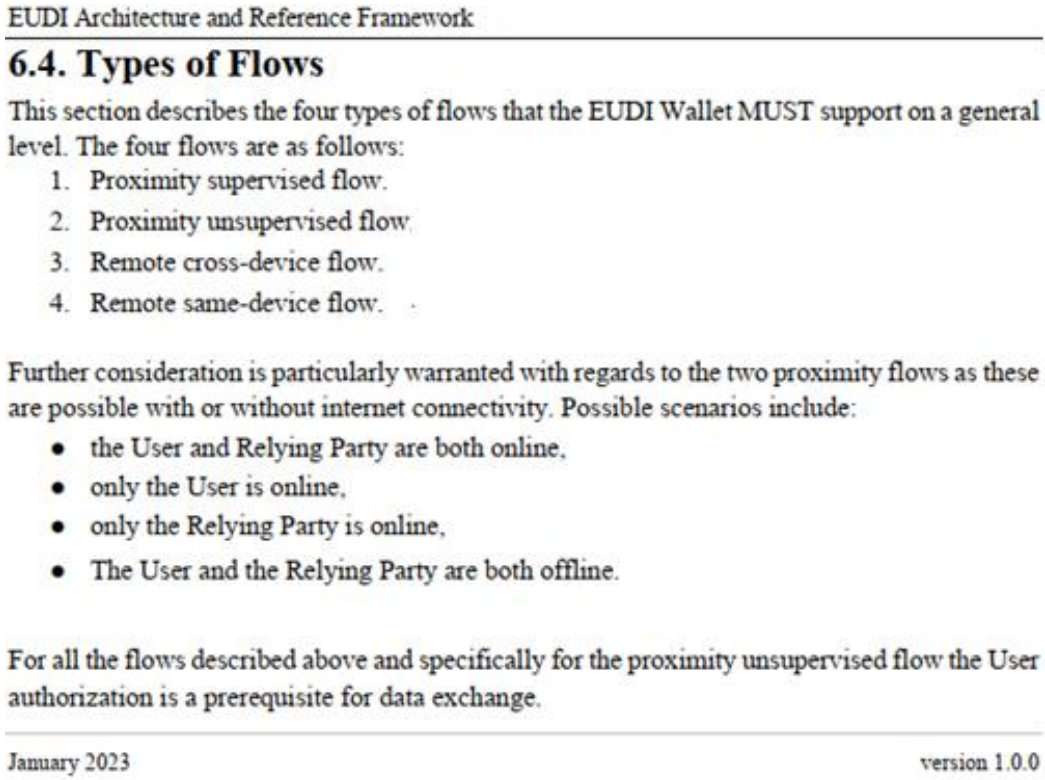
Az eIDAS 1.0 szerinti interfészeken keresztül is lehetett

- adatokat lekérdezni (KAÜ, eSzemélyi okmány);
- minősített elektronikus aláírást létrehozni (eSzemélyi okmány);

online folyamatoknál. (és offline?)

offline User + offline Relying Party
online User + offline Relying Party
offline User + online Relying Party
online User + online Relying Party

***online = temporarily/permanently online**



EUDI Architecture and Reference Framework

6.4. Types of Flows

This section describes the four types of flows that the EUDI Wallet MUST support on a general level. The four flows are as follows:

1. Proximity supervised flow.
2. Proximity unsupervised flow.
3. Remote cross-device flow.
4. Remote same-device flow.

Further consideration is particularly warranted with regards to the two proximity flows as these are possible with or without internet connectivity. Possible scenarios include:

- the User and Relying Party are both online,
- only the User is online,
- only the Relying Party is online,
- The User and the Relying Party are both offline.

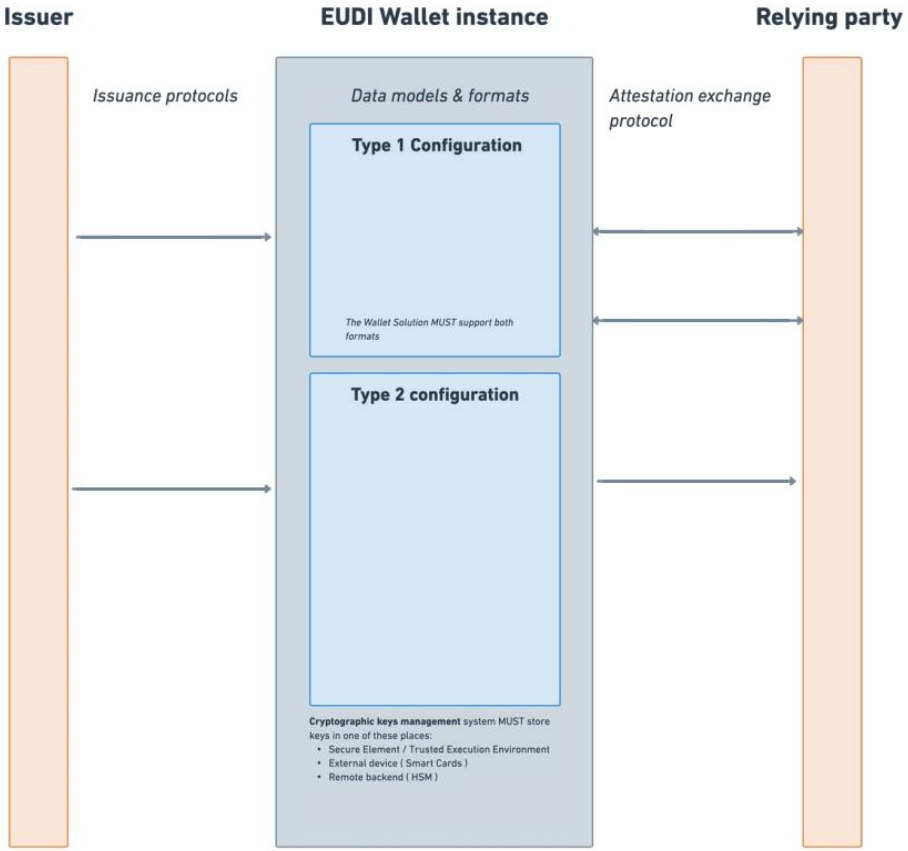
For all the flows described above and specifically for the proximity unsupervised flow the User authorization is a prerequisite for data exchange.

January 2023 version 1.0.0

MELASZ

A jogszabálytervezet szerint mi a wallet?

'European Digital Identity Wallet' is an electronic identification means that allows the user to store identity data, electronic attestations of attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals;



Az offline folyamatok támogatása és vele a központi jóváhagyás/ellenőrzés kiváltása a saját döntéssel (consent, revocation/up-to-dateness check), illetve az, hogy az adatot kérő nem csak jogi személy, hanem természetes személy is lehet azt jelzi, hogy az eIDAS 2.0 egyben műszaki megoldást szolgáltat a GDPR számára is (a 20. cikk szerinti "Az adathordozhatósághoz való jog" megvalósítására sosem született egységes specifikáció ezért rendszerenként eltér a lekérdezett adatok struktúrája, így ráépülő elemző megoldások sem készíthetők).

4.1.10. Relying Parties

Relying Parties are natural or legal persons [...].

/ARF, 2023-01-26/

Article 20

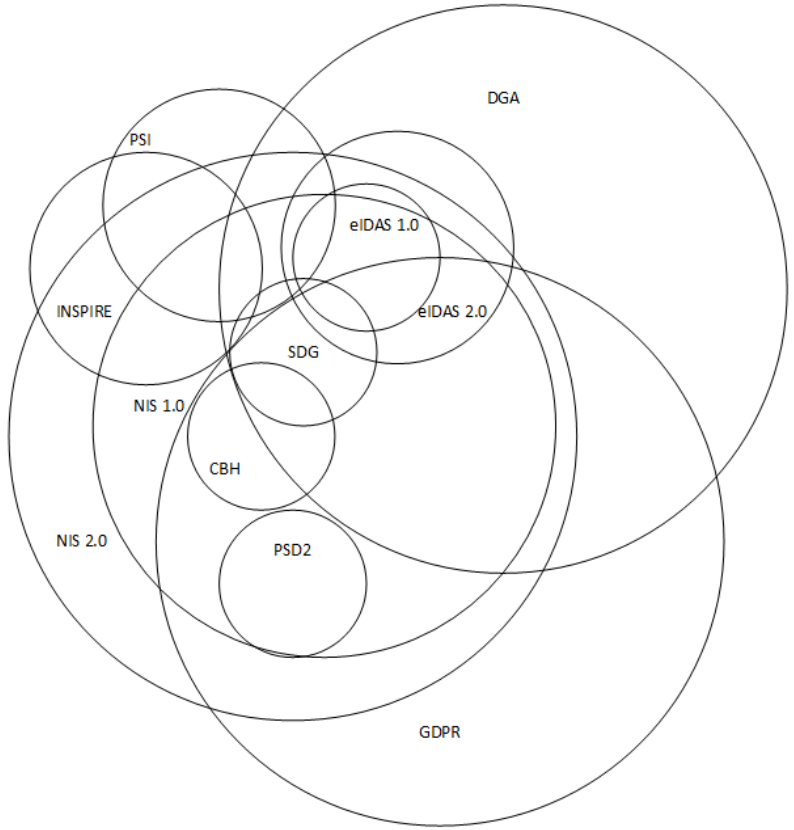
Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller [...].

/GDPR, 2018-05-25/

MELASZ

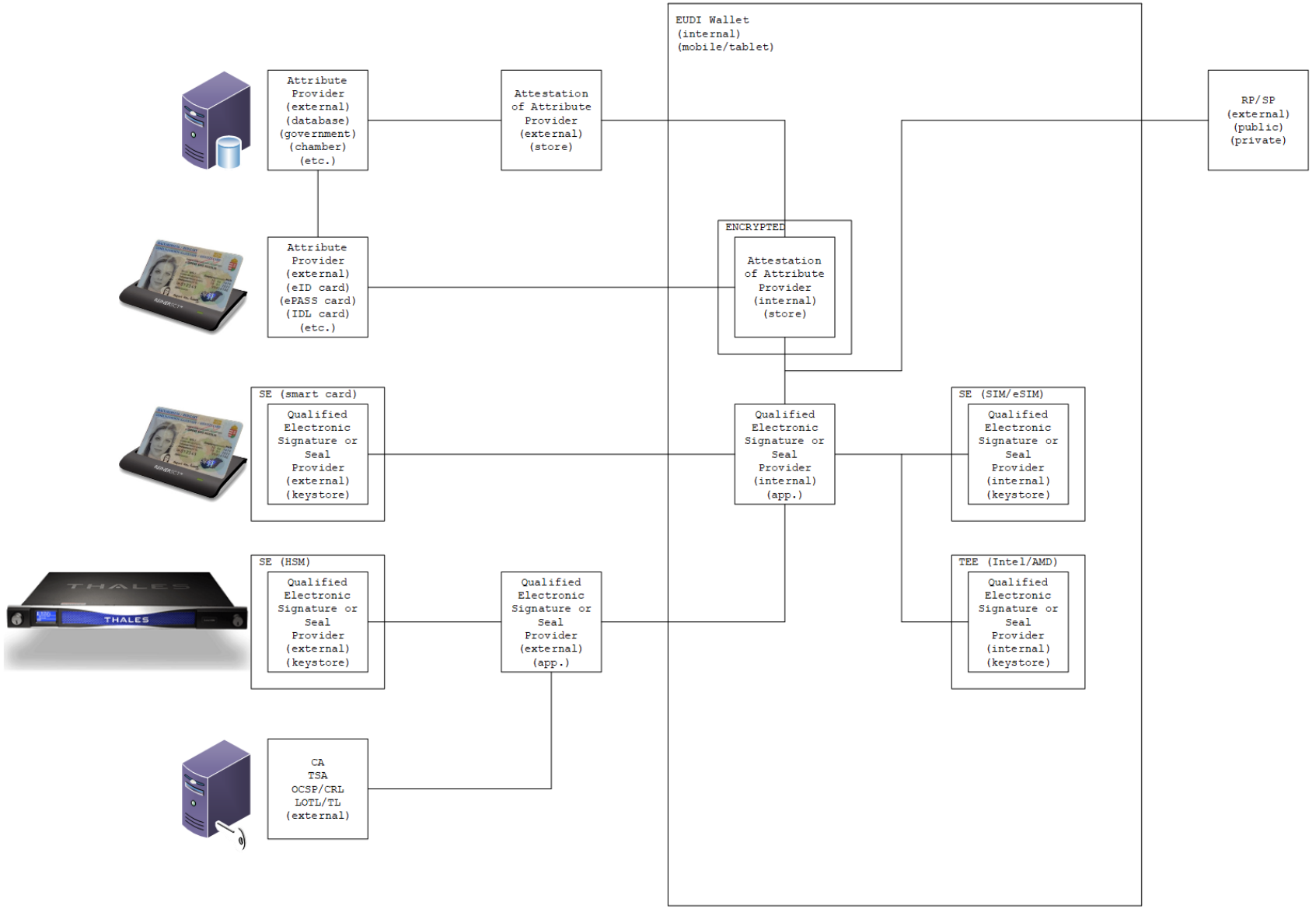
Az eIDAS 2.0 által elérhető adatok köre hogy viszonyul a többi EU-s adatszolgáltatási jogszabályhoz? (Venn-diagram)



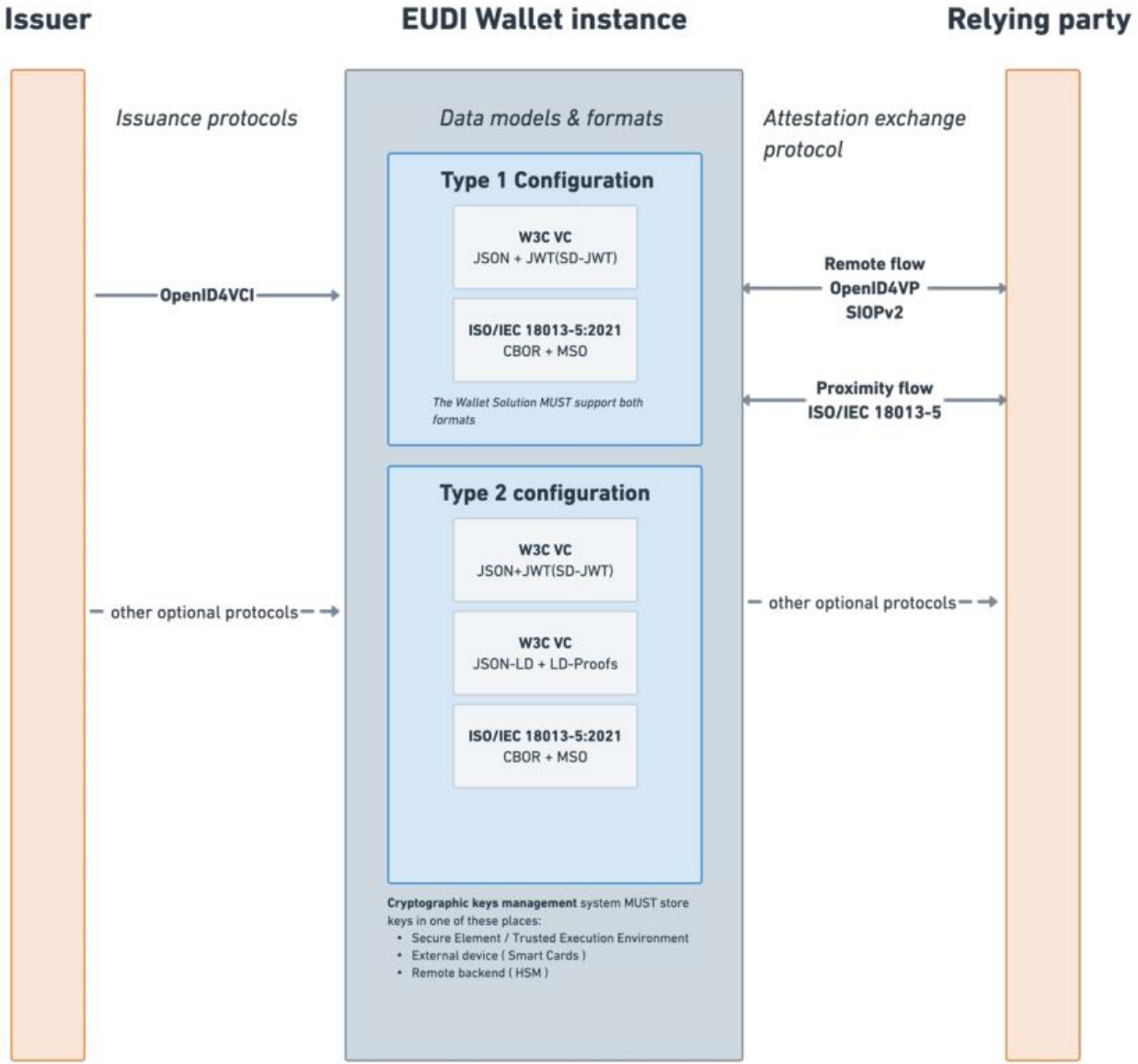
based on?			about who?	how?	what type of?	by who?
INSPIRE	Directive	2007/2/EC	Member State	non-anonymized	geospatial data	by public attribute provider
CBH	Directive	2011/24/EU	natural person	non-anonymized	medical record (patient summary)	by public/private attribute provider (healthcare provider, accredited by Government of Member State)
eIDAS 1.0	Regulation	(EU) No 910/2014	natural/legal person	non-anonymized	8+10+2 attributes	by public/private attribute provider (accredited by Government of Member State)
PSD2	Directive	(EU) 2015/2366	natural/legal person	non-anonymized	account information	by private attribute provider (AISP, accredited by Central Bank of Member State)
GDPR	Regulation	(EU) 2016/679	natural person	non-anonymized	personal data	by private attribute provider
NIS 1.0	Directive	(EU) 2016/1148	natural/legal person	non-anonymized	critical entity-stored attributes	by public/private attribute provider (based on restrictions)
SDG	Regulation	(EU) 2018/1724	natural/legal person	non-anonymized	life event attributes	by public/private attribute provider (accredited by Government of Member State)
PSI	Directive	(EU) 2019/1024	natural/legal person	anonymized	government-stored attributes	by public/private attribute provider (accredited by Government of Member State)
DGA	Regulation	(EU) 2022/868	natural/legal person	non-anonymized	government-stored attributes	by public/private attribute provider (data intermediation service, accredited by Government of Member State)
NIS 2.0	Directive	(EU) 2022/2555	natural/legal person	non-anonymized	critical entity-stored attributes	by public/private attribute provider (based on restrictions)
eIDAS 2.0	???		natural/legal person	non-anonymized	attestations and attributes	by public/private attribute provider ((Q)EAA+EUDIW, accredited by Government of Member State)

eIDAS 2.0 – EUDI wallet

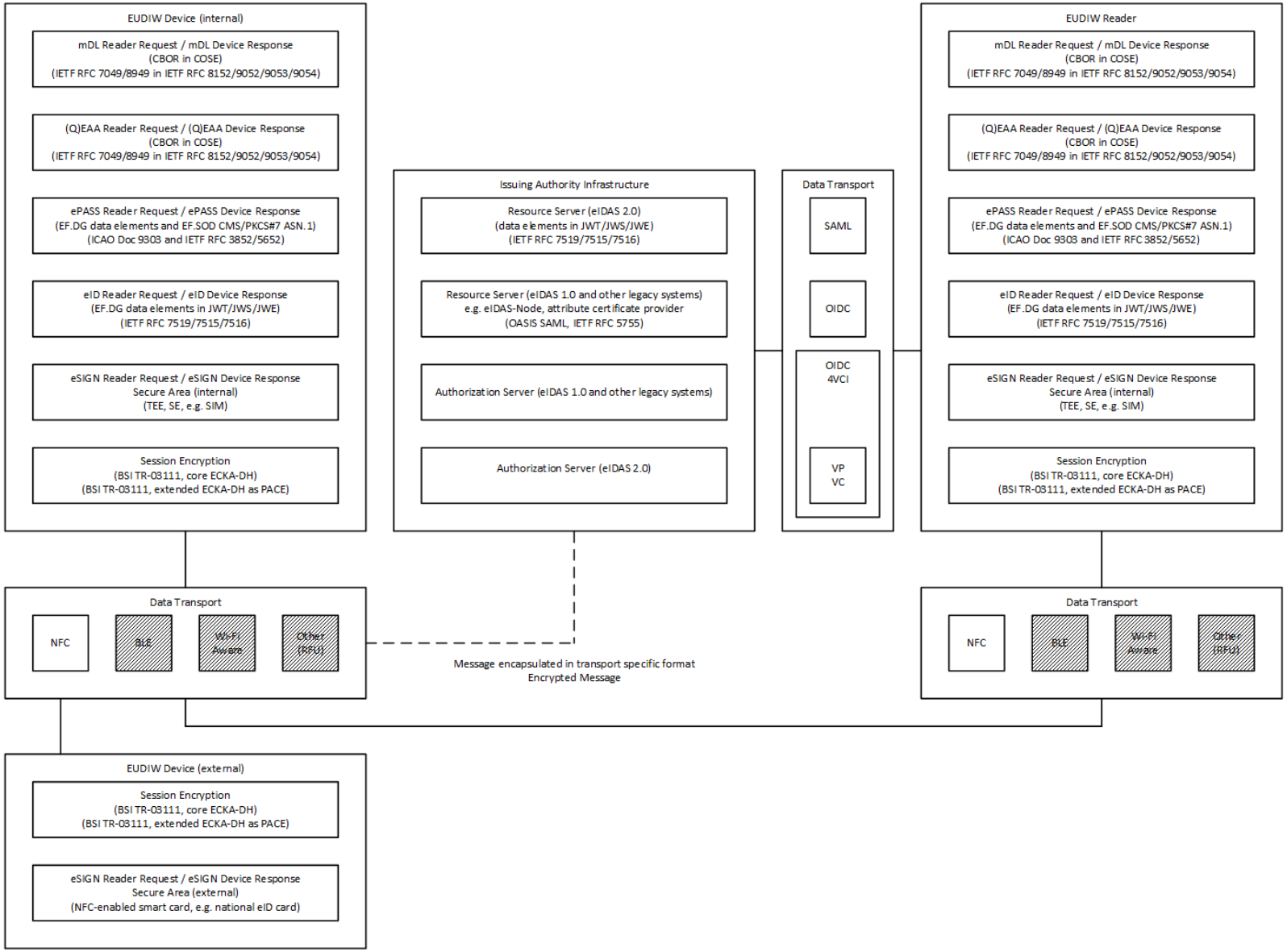
MELASZ



eIDAS 2.0 – EUDI wallet



eIDAS 2.0 – EUDI wallet



Támogatni kell az:

eIDAS 1.0 modellt

- eIDAS node (SAML protokoll, Assertion XML üzenetek)
- national eID card (OIDC protokoll, JWT JSON üzenetek)

eIDAS 2.0 modellt

- EUDI wallet (OIDC4VCI protokoll, Verifiable Credential JSON vagy CBOR üzenetek)

[...] there may be a need for additional trusted components which are not part of that application [...]

- *Re-use of backend systems*.
- *Re-use of decentralised identity infrastructure*.

/ARF, 2023-01-26/

The existing infrastructures involved in the processes described above includes: [...]

- *relying parties, brokers, proxies including eIDAS nodes and other national eID brokers and gateways;*
- *notified electronic identity means*.

[...] interfaces between the EUDI Wallet and the Member States corresponding infrastructures shall be established

/ARF, 2022-02-22/

Támogatni kell az:

eIDAS 1.0 modellt

- Commission Implementing Decision (EU) 2015/1506 (XAdES, CAdES, PAdES, ASiC) (LoA High)

eIDAS 2.0 modellt

- EUDI wallet (JAdES) (LoA High)

Signature formats-1

EUDI Wallet Solution [...] support signature and encryption formats in accordance with JOSE(JWT) specifications.

MUST – Type 1 configuration (LoA High)

MAY – Type 2 configuration

/ARF, 2023-01-26/

XAdES Baseline Profile

CAdES Baseline Profile

PAdES Baseline Profile

Associated Signature Container Baseline Profile

/Commission Implementing Decision (EU) 2015/1506, 2015-09-08/

MELASZ

Támogatni kell az:

eIDAS 1.0 modellt

- eIDAS – Cryptographic requirements for the Interoperability Framework (RSASSA-PSS, ECDSA-NIST/Brainpool)

eIDAS 2.0 modellt

- ???quantum-safe??? (CRYSTALS-DILITHIUM, FALCON, SPHINCS+)

	Public-Key Encryption Key-Encapsulation Mechanism		Digital Signature	
	Winner	Round 4	Winner	Round 4
code-based		BIKE Classic McEliece HQC		
lattice-based	CRYSTALS-KYBER		CRYSTALS-DILITHIUM FALCON	
isogeny-based		SIKE		
multivariate				
zero-knowledge				
hash-based			SPHINCS+	

/NIST PQC, 2022-07-05/

ARF (Architecture and Reference Framework)

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases

ETSI TS 119 432 (OASIS DSS XML-based and CSC JSON-based messages)

Protocols for remote digital signature creation

ETSI TS 119 461

Policy and security requirements for trust service components providing identity proofing of trust service subjects

ETSI TS 119 462

Wallet interfaces for trust services and signings

ETSI TS 119 471

Policy and Security requirements for Attribute Attestation Services

ETSI TS 119 472

Profiles for Attribute Attestations