How FIDO can be used for the EUDI Wallet

Presentation at ENISA Trust Services Forum 2022

October 27, 2022

Rayissa Armata, Senior Head Of Regulatory Affairs at IDnow
Sebastian Elfors, Senior Architect at IDnow

Agenda

- Introduction to the FIDO Alliance

- FIDO solutions for the EUDI Wallet

- FIDO white papers on eIDAS

- Questions

Introduction to the FIDO Alliance

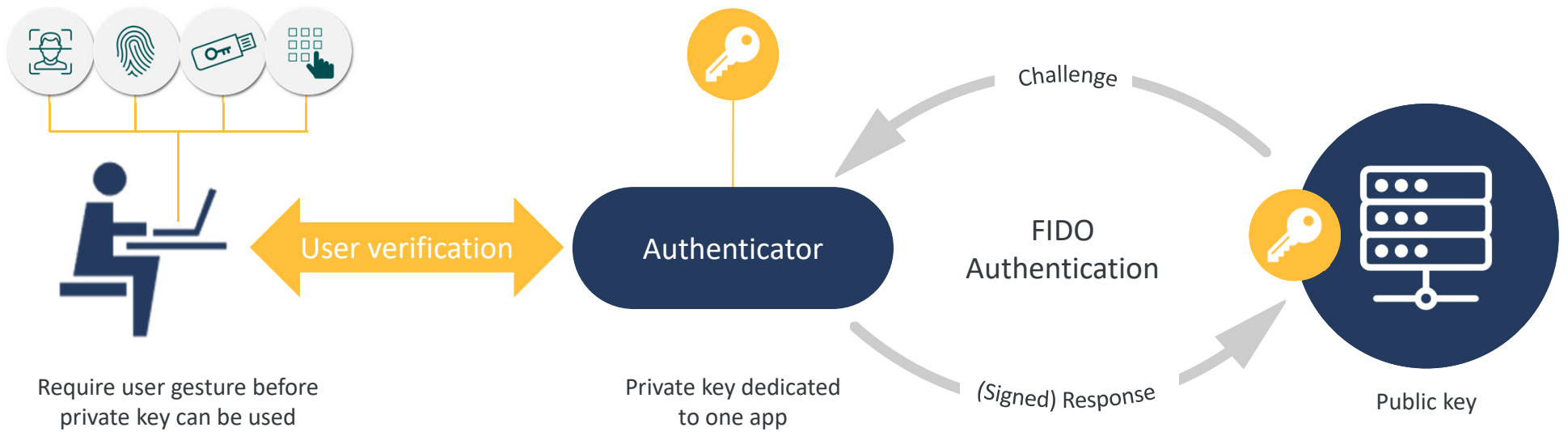# Backed by global tech leaders

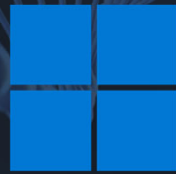amazon | AMERICAN EXPRESS | Apple | Bank of America | CVS Health | egis Technology

FEITIAN WE BUILD SECURITY | Google | HYPR | IDEMIA | Infineon | ING | intel

JUMIO | LastPass | Lenovo | LINE | mastercard | Meta | Microsoft

nok nok | NTT docomo | OneSpan Be bold. Be secure. | onfido | PayPal | Qualcomm | RAON

RSA | SAMSUNG | Synaptics | THALES | Transmit security | TRUSONA | TrustKey SOLUTIONS

USAA | US bank | VISA | vmware | WELLS FARGO | YAHOO! JAPAN | yubico

| + Sponsor members | + Associate members | + Liaison members | + Government members |

fido ALLIANCE

FIDO Authentication: How it works

User verification

Authenticator

FIDO Authentication

Challenge

(Signed) Response

Require user gesture before
private key can be used

Private key dedicated
to one app

Public key

Browser and OS Support = Endpoint Ubiquity

FIDO in Europe

- Active FIDO European Working Group – with 62 members

- The FIDO Alliance is an official liaison member with ETSI since 2021

- Launched an EUDI Wallet Subgroup last year – in response to the eIDAS2 proposal

- Explore how FIDO authentication can be utilized for eIDAS2 and the EUDI Wallet

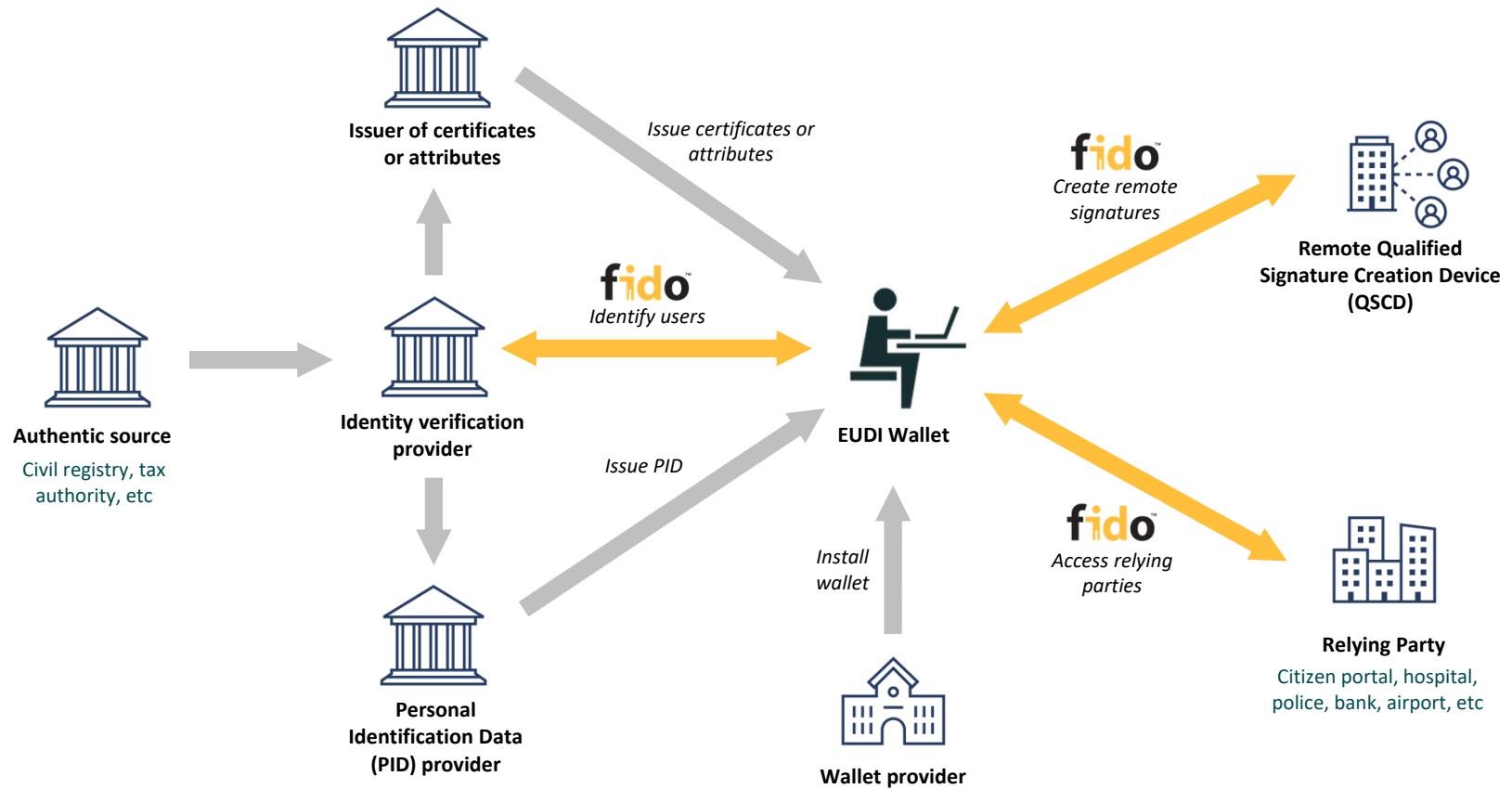- Several meetings held with ETSI, W3C, ENISA, ministries, universities and experts
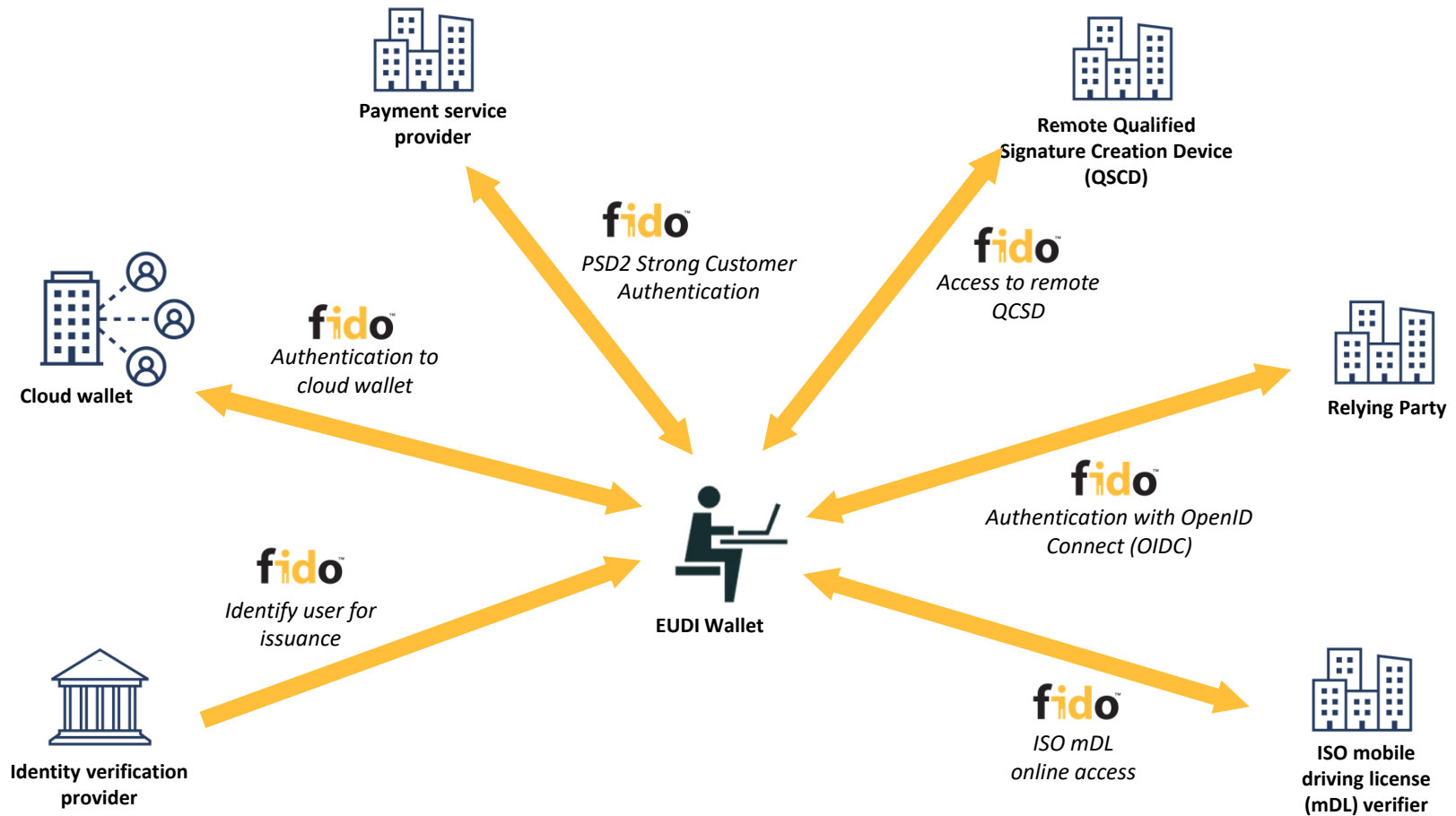
FIDO solutions for the EUDI Wallet
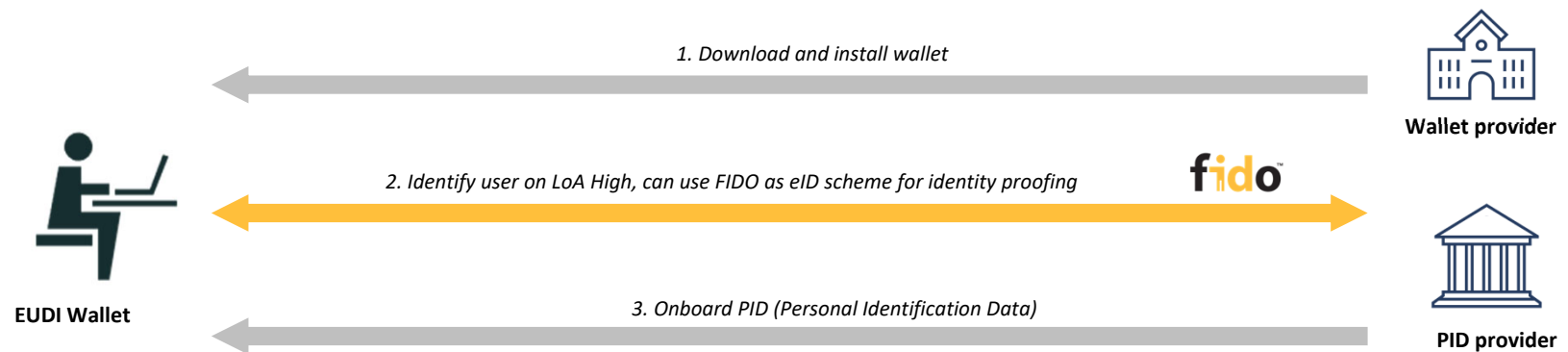
EUDI Wallet Ecosystem

FIDO use cases for the EUDI Wallet

Issuance of EUDI Wallet

eIDAS2 Article 6a §6:

"The European Digital Identity Wallets shall be issued under a notified <u>electronic identification scheme</u> of level of assurance 'high'."

1. Download and install wallet

Wallet provider

fido

2. Identify user on LoA High, can use FIDO as eID scheme for identity proofing

EUDI Wallet

3. Onboard PID (Personal Identification Data)
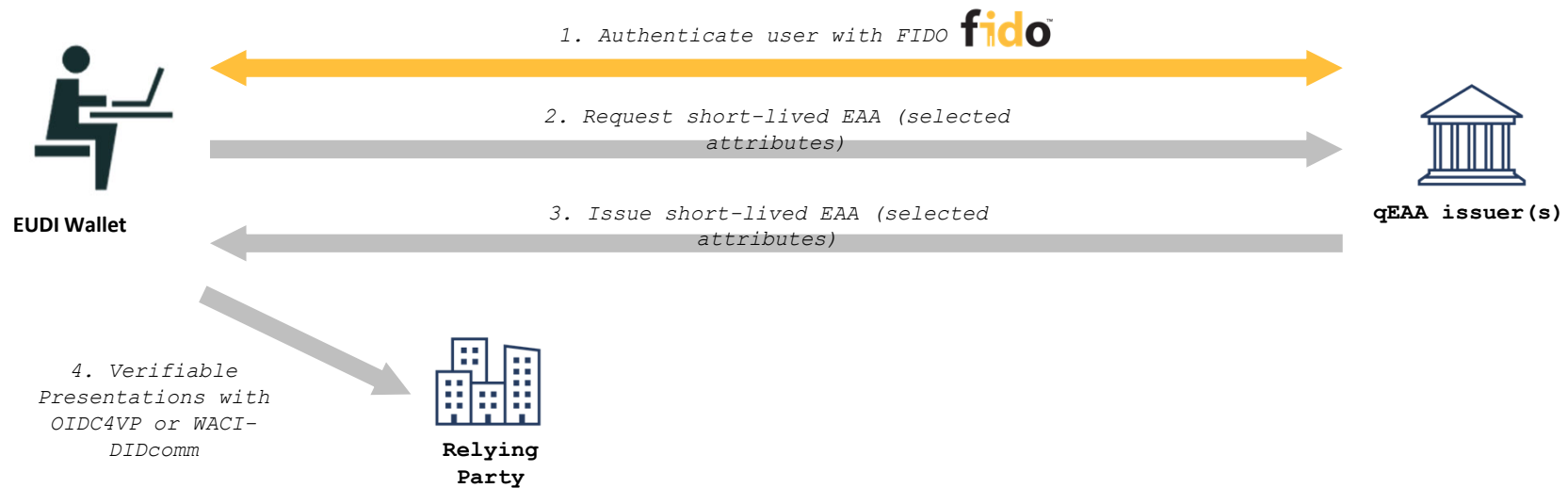
PID provider

- CEN/TC224/WG20 introduces the concept of EUDI Wallet Personal Identification Data (PID) onboarding

- ETSI TS 119 461 describes remote identity proofing

- FIDO allows for the authentication part of identity proofing as eID scheme at Level of Assurance (LoA) High

- Examples: FIDO is certified as national eID schemes on LoA High in the Czech Republic and Norway

Selective disclosure with short-lived EAAs

> **eIDAS2 Recital 29:**
>
> *"The European Digital Identity Wallet should technically enable the <u>selective disclosure</u> of attributes to relying parties."*

1. Authenticate user with FIDO fido

EUDI Wallet

2. Request short-lived EAA (selected attributes)

3. Issue short-lived EAA (selected attributes)

qEAA issuer(s)

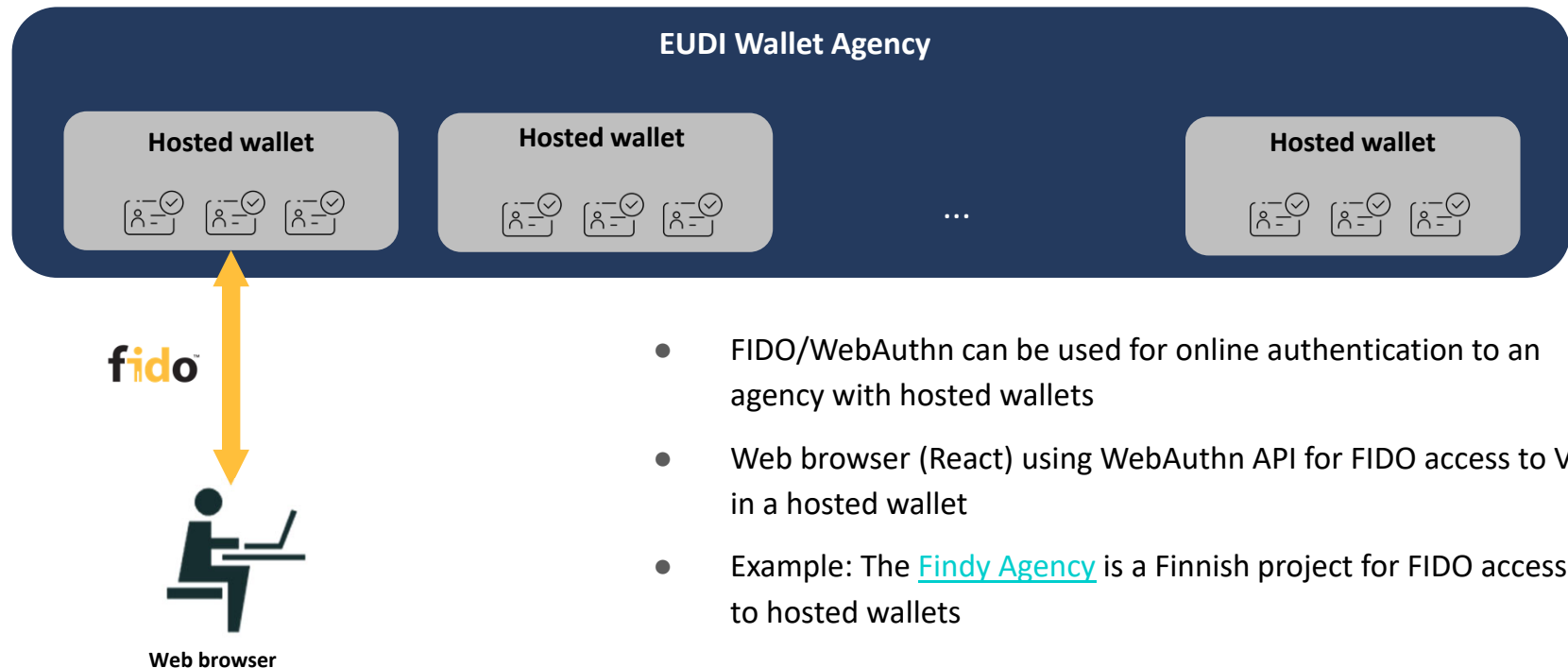*4. Verifiable Presentations with OIDC4VP or WACI-DIDcomm*

Relying Party

- Issuance of short-lived EAAs with selected attributes can be used for selective disclosure

- FIDO can be used for issuance of EAAs according to eIDAS2 Article 24 §1a (eID scheme)

- The Kent University VC-FIDO integration uses FIDO for issuance of short-lived EAAs
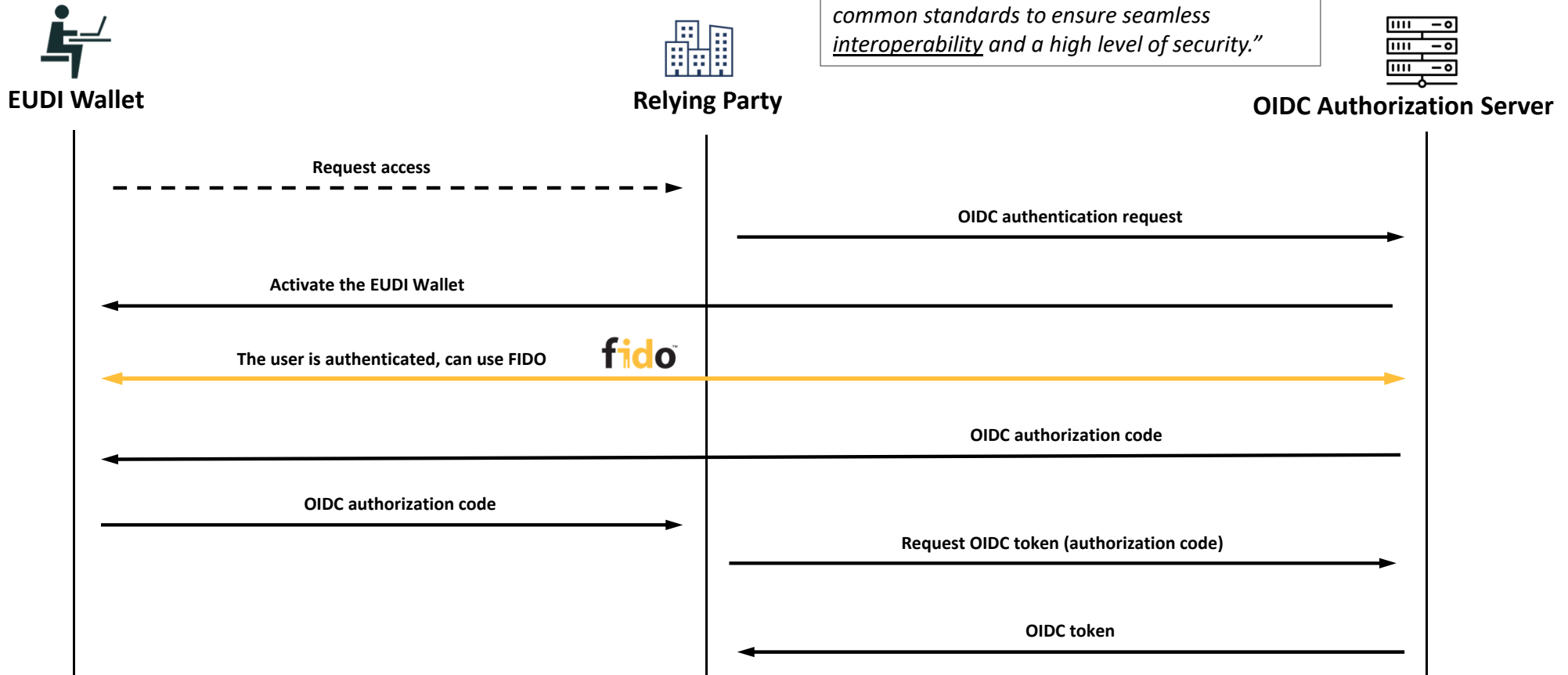
Access to cloud-based EUDI Wallet

eIDAS2 Recital 11:

"European Digital Identity Wallets should ensure the highest level of security for the personal data used for authentication irrespective of whether such data is stored locally or on _cloud-based solutions..._"

- FIDO/WebAuthn can be used for online authentication to an agency with hosted wallets

- Web browser (React) using WebAuthn API for FIDO access to VC in a hosted wallet

- Example: The Findy Agency is a Finnish project for FIDO access to hosted wallets
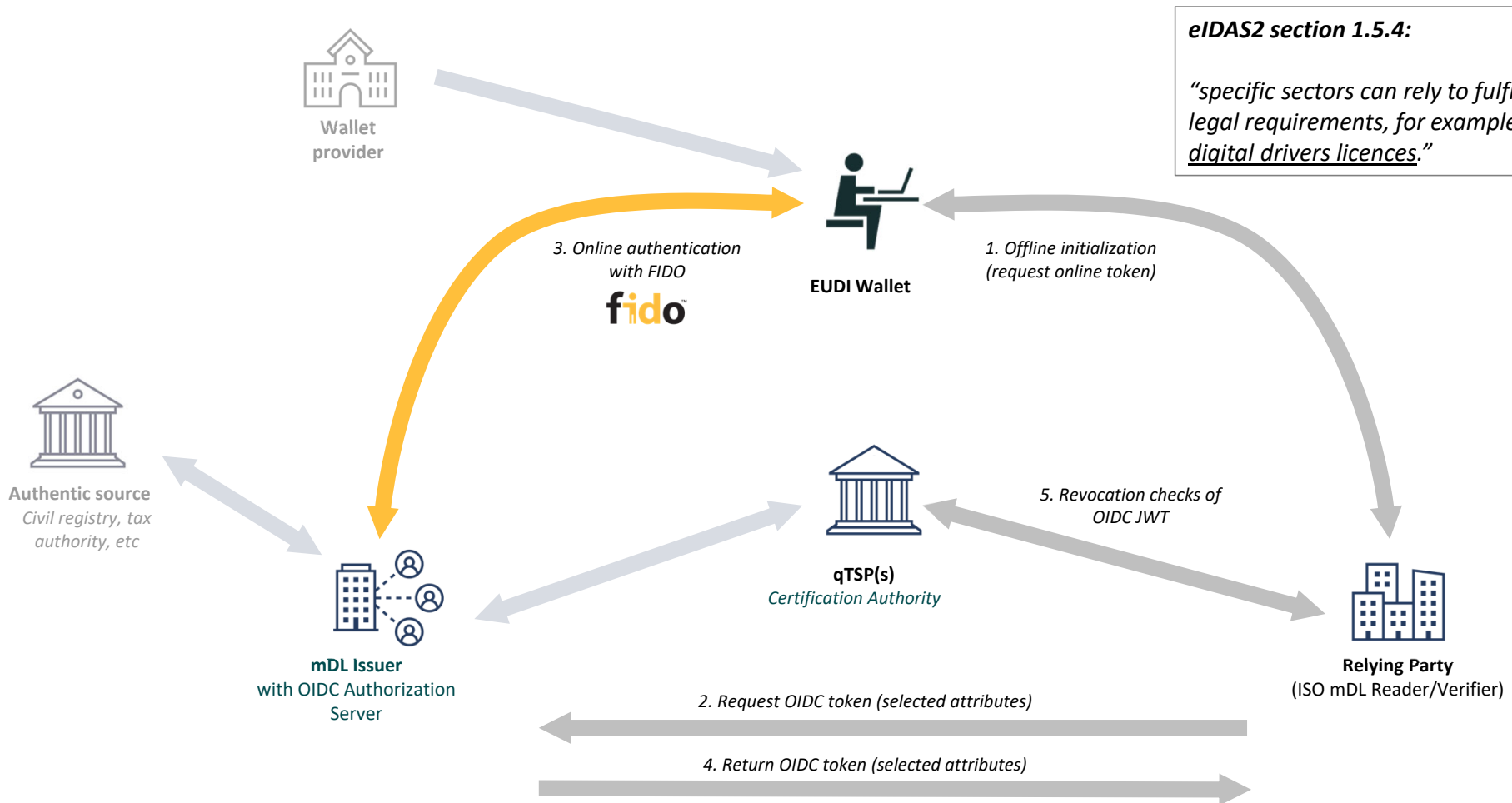
Interoperability with OpenID Connect (OIDC)

eIDAS2 Recital 9:

"European Digital Identity Wallets relying on common standards to ensure seamless _interoperability_ and a high level of security."

EUDI Wallet

Relying Party

OIDC Authorization Server

Request access →

OIDC authentication request →

← Activate the EUDI Wallet

The user is authenticated, can use FIDO **fido**™ ←→

← OIDC authorization code

OIDC authorization code →

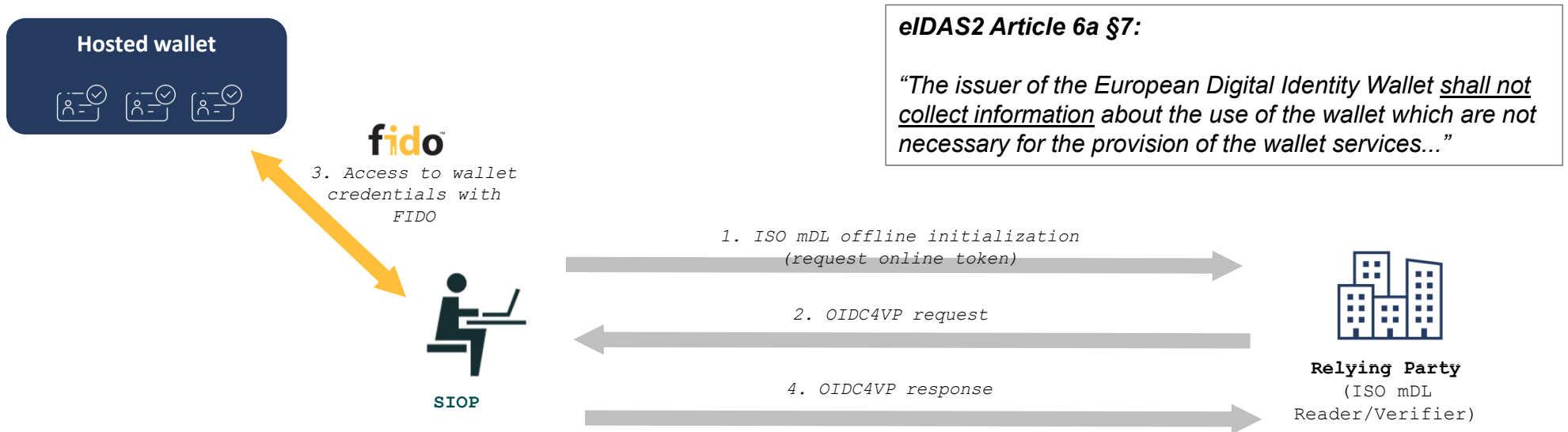Request OIDC token (authorization code) →

← OIDC token

Online OIDC authorization for ISO 18013-5 (mDL)

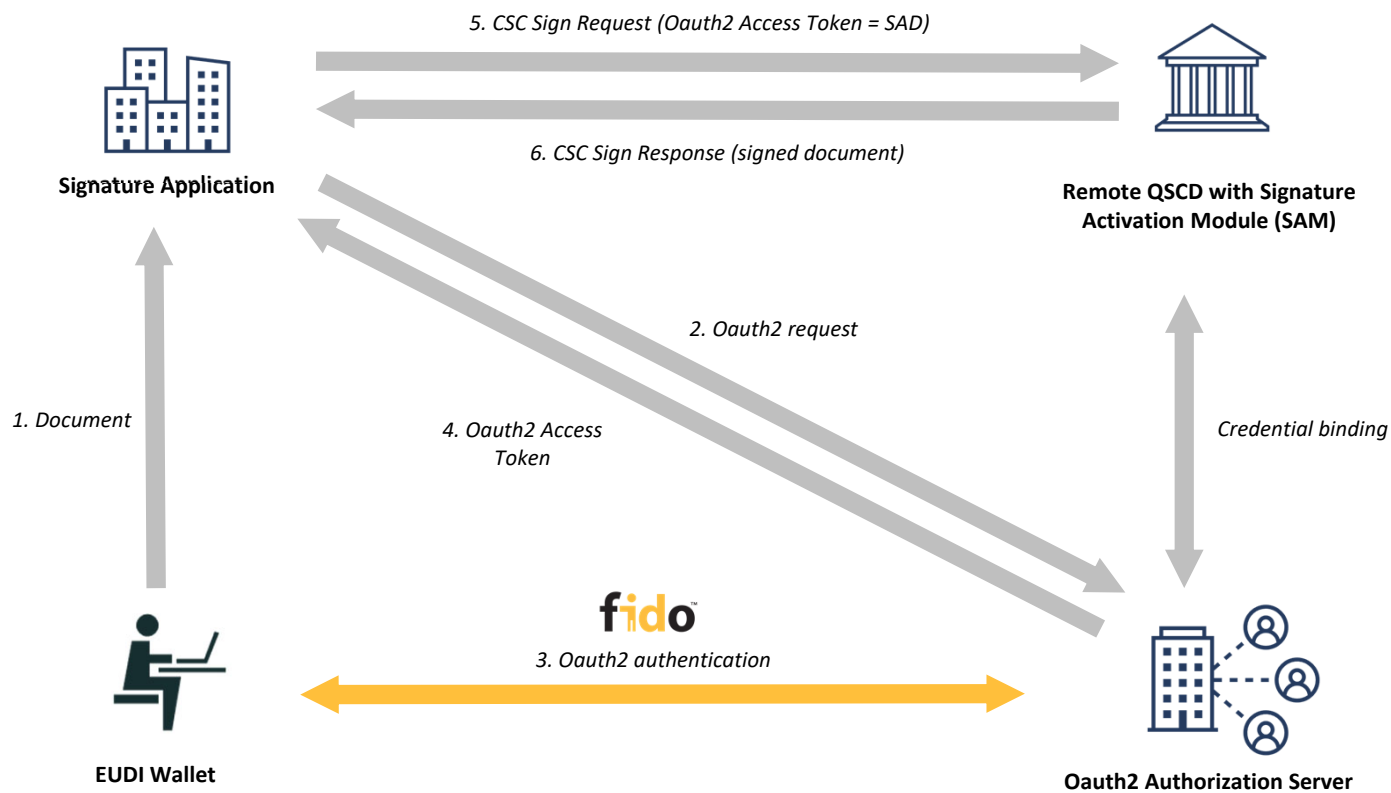

eIDAS2 section 1.5.4:

"specific sectors can rely to fulfil sector specific legal requirements, for example related to _digital drivers licences_."

Wallet provider

EUDI Wallet

3. Online authentication with FIDO

fido

1. Offline initialization (request online token)

Authentic source
Civil registry, tax authority, etc

qTSP(s)
Certification Authority

5. Revocation checks of OIDC JWT

mDL Issuer
with OIDC Authorization Server

Relying Party
(ISO mDL Reader/Verifier)

2. Request OIDC token (selected attributes)

4. Return OIDC token (selected attributes)

ISO mDL with ISO 23220-4

Hosted wallet

fido

3. Access to wallet credentials with FIDO

SIOP

eIDAS2 Article 6a §7:

"The issuer of the European Digital Identity Wallet <u>shall not collect information</u> about the use of the wallet which are not necessary for the provision of the wallet services..."

1. ISO mDL offline initialization (request online token)

2. OIDC4VP request

4. OIDC4VP response

Relying Party
(ISO mDL Reader/Verifier)

- eIDAS2 Article 6a §7 stipulates privacy for the user

- Self-Issued OpenID Connect Provider (SIOP) runs at the user's device

- OpenID Connect for Verifiable Presentations (OIDC4VP) used for access to relying parties

- ISO 23220-4 specifies SIOP2 and OIDC4VP for user controlled ISO mDL

- FIDO can be used for access to cloud hosted wallet (or device wallet)
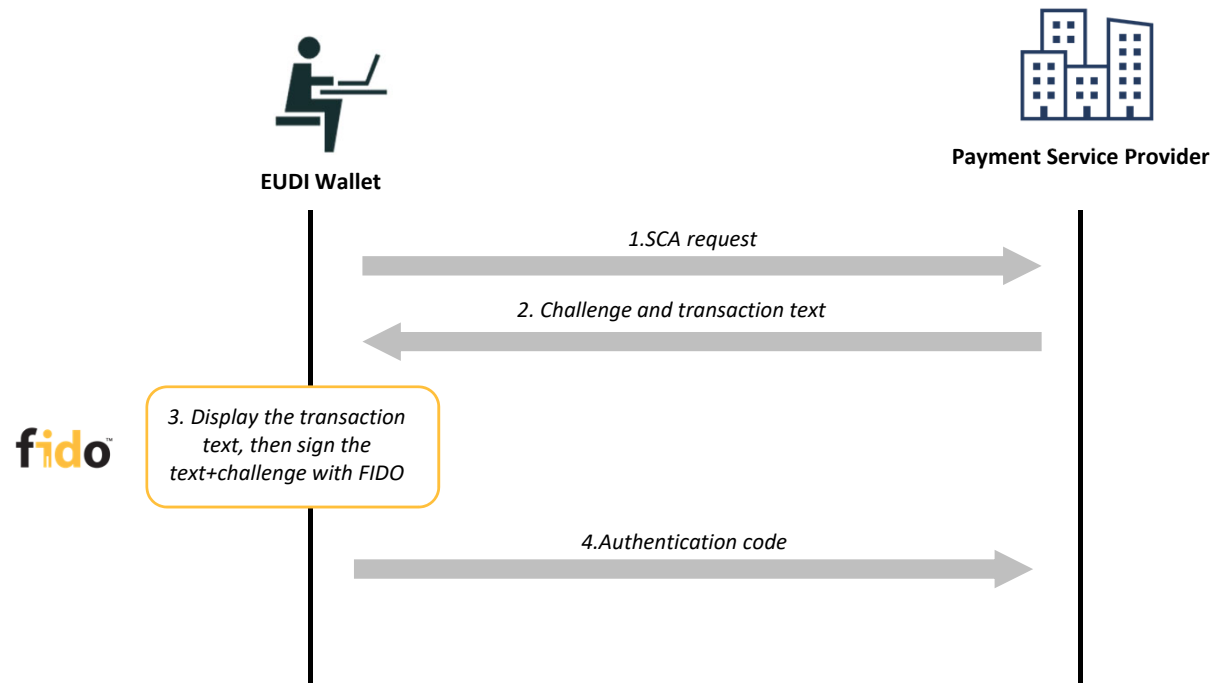
Authentication for remote signing

5. CSC Sign Request (Oauth2 Access Token = SAD)

6. CSC Sign Response (signed document)

Signature Application

Remote QSCD with Signature Activation Module (SAM)

2. Oauth2 request

1. Document

4. Oauth2 Access Token

Credential binding

3. Oauth2 authentication

EUDI Wallet

Oauth2 Authorization Server

eIDAS2 Article 29a:

"Requirements for a qualified service for the management of remote electronic signature creation devices..."

- CEN standards EN 419 241 and EN 419 221 specify:
  - Signature Activation Module (SAM)
  - Signature Activation Data (SAD)
- Cloud Signature Consortium (CSC) API uses Oauth2 to create SAD
- FIDO can be used for Oauth2 authentication

PSD2 Strong Customer Authentication (SCA)

> **eIDAS2 Recital 31:**
>
> *"support the fulfilment of <u>strong customer authentication</u> requirements for account login and initiation of transactions in the field of payment services...."*

EUDI Wallet

Payment Service Provider

1.SCA request →

← *2. Challenge and transaction text*

3. Display the transaction text, then sign the text+challenge with FIDO

4.Authentication code →

- Compliance with EU Payment Services Directive 2 (PSD2) needed

- Strong Customer Authentication (SCA) for Dynamic Linking required

- FIDO can be used for PSD2 SCA

- FIDO Alliance has published white papers on PSD2 deployments

FIDO white papers on eIDAS

Download the FIDO white papers on eIDAS

Introduction of FIDO & eIDAS Services

https://fidoalliance.org/white-paper-introduction-of-fido-eidas-services/

Using FIDO with eIDAS Services

https://fidoalliance.org/white-paper-using-fido-with-eidas-services/

FIDO Alliance white paper on the EUDI Wallet coming soon

Questions?