EUDI and Standards
Why is the EU Digital Identity needed?
Why is the EU Digital Identity needed?

Consumers and services have moved on

Expectations of consumers have changed; mobile apps and digital services are becoming the norm.

A shift away from identity alone and more emphasis on the provision of trusted data.

A shift towards more user centric identity solutions allowing users to control all aspects of their digital identity and protect personal data.
Why is the EU Digital Identity needed?

**A digital identity for all EU citizens**

The reach of digital ID was not realised under the first eIDAS Regulation.

Ensures that all Member States must provide a digital identity to their citizens.

80% of citizens should be able to use a digital ID solution to access key public services by 2030.

Consumers should be able to access services online without having to use private platforms or unnecessarily sharing personal data.
The eIDAS Regulation

**Legal constructs and technical specifications**

The Regulation includes a number of Implementing Acts and technical specifications that support cross-border interoperability and high levels of trust in digital identity and e-services.

This includes:
- Levels of Assurance
- Interoperability (e.g. data schema and technical protocols)
- E-signature specifications (e.g. Qualified Electronic Signatures)
National Enrolment and Identity Proofing

Each Member State is responsible for verifying the identity of citizens and residents

For an individual to obtain a digital identity they must first provide evidence of their real-world identity that can be verified.

In general identity verification should:

- Check the quality of evidence provided
- Check that evidence is valid and/or genuine
- Check that the identity has existed over time
- Check for risk of fraudulent activity
- Verify that the identity belongs to the person making the claim
The latest version of eIDAS includes identity wallets
Overarching requirements on the EUDI Wallet

The EUDI Wallet:

- is an **electronic identification means**
- is able to **request, select, combine, store, delete** and **present**
  electronic attestation of attributes (**EAAs**) and person identification data (**PID**) to Relying Parties
- enables the user to create (**local or remote**) qualified electronic signature (**QES**)
Overarching requirements on the EUDI Wallet

The EU Digital Identity Wallet will be:

- **made available to anyone who wants to use it:** Any EU citizen, resident, and business in the EU who would like to make use of the EU Digital Identity will be able to do so.

- **used widely:** EU Digital Identity Wallets will be used as a way to identify users when providing them with access to public and private digital services across the EU.

- **controlled by users:** The EU Digital Identity Wallets will enable people to choose and keep track of their identity, data and certificates which they share with third parties. Anything which is not necessary to share will not be shared.
The Architecture Reference Framework

The core technical requirements for the EUDI Wallet

**EUDI Wallet ecosystem** – Trust Framework, roles and responsibilities

**Person identification data (PID) and electronic attestations of attributes (EAA)**

**Data sets & formats** – e.g. credential binding and credential formats

**Functional requirements of the EUDI Wallet** e.g. Wallet lifecycle & Validity management

**Business processes and EUDI Wallet use cases**
- Wallet as an eID means – online PID presentation
- Mobile driving licence

**Certification of EUDI Wallet** e.g. Legal requirements and scope
The Architecture Reference Framework

Developing in the open

The technical Architecture and Reference framework is being developed in GitHub.

The ARF will provide the specifications needed to develop an interoperable EUDI Wallet Solution based on common standards and practices.
Large Scale Pilots (LSPs)

To test digital identity wallets in real-life scenarios

The LSPs span different sectors such as such as healthcare, financial services, education and transport.

They will utilise a reference wallet provided by the European Commission.

Over 250 private companies and public authorities across 25 Member States and Norway, Iceland, and Ukraine will participate.

Potential: eGov services, Bank Account Opening, SIM registration, mDL, Qualified Signature

Nobid: authorisation of payments for products and services by the wallet user/holder

DC4EU: educational and professional qualifications, European Health Insurance Card.

EWC: Digital Travel Credentials, Organisational Digital Identities
EU Digital Identity Wallets Certification

A greater emphasis on certification

EUDI Wallet Issuers must request (select, contract) a designated Certification Assessment Body (CAB) to assess and certify the conformity of their Wallet against the requirements of the eIDAS Regulation.

EUDI Wallet Issuers will be responsible for ensuring compliance with the applicable requirements for EUDI Wallets, in particular the relevant specifications, functional and non-functional as well as security and personal data protection / processing requirements.
Building on standards

**Ensuring interoperability and ease of implementation**

The ARF toolbox specifications identify the core standards upon which the EU Digital Identity Wallet will be built.

- W3C Verifiable Credentials
- OpenIDVCI / OpenID4VP
- ISO/IEC 18013-5:2021 (for mDL)
The EUDI Wallet

OpenID4VP

Other optional protocols
e.g. ISO 18013

PID issued at LoA High

PID issued at LoA High

(Q)EAA

Mobile DL

PID

Binding / AuthN

QES

ISO 18013-5

Proximity Flow

OpenID4VP

OpenID4VP

PID issued at LoA High

eID Means =>
1) PID bound to the citizen
2) strong authenticator
3) certified wallet

PID issued at LoA High
The EUDI Wallet

- OpenIDVCI
  - PID issued at LoA High

- Other optional protocols
  - e.g. ISO 18013

- OpenID4VP

- ISO 18013-5
  - Proximity Flow

- Mobile DL

(Q)EAA
- Binding / AuthN

PID

Other optional protocols supported, for example, Mobile DL.
The EUDI Wallet

- OpenIDVCI
  - PID issued at LoA High

- Other optional protocols
  - e.g. ISO 18013

- PID and (Q)EAA presentation online and offline.

- PID
  - Binding / AuthN

- (Q)EAA
  - QES

- Mobile DL

- ISO 18013-5
  - Proximity Flow
Indicative wallet experiences
Online identity data sharing and account creation

User visits RP online service

Chooses the wallet to use

Wallet resolves request and user authenticates to wallet

User confirms or consents to sharing

Wallet communicates data response to RP

RP online service uses the data
Offline identity data presentation

1. Citizen meets RP (representative) in person and asks for data
2. Citizen selects requested information
3. Wallet communicates selected data to RP
4. RP compares portraits with Citizen’s face
5. Scanning and/or visual inspection
Offline (interactive) identity data presentation

Citizen meets RP (representative) in-person

RP requests data from wallet

Citizen authenticates to wallet

Citizen confirms consent to sharing

Wallet communicates data response to RP

RP compares portrait with user's face
Wallet examples

Trust mark is attached to the gyro inside the control system in the smartphone

Animated background for heightened security

A timestamp to be sure the animation/gyro-effect is neither a video nor is manipulated
Thank you