Get to know ID used across borders in the European Union
An ID4D Webinar Series

A European Framework for Decentralized Digital Identity Wallets
The European Digital Identity Framework

Bogdan STEFAN
DG CONNECT, European Commission
Bogdan.Stefan@ec.europa.eu
Agenda

1. The state of play
2. The European Digital Identity Framework
3. New Trust Services +
4. Next steps
The state of play
Challenges to the cross-border use of national eIDs

Four factors hindering cross-border authentication under the eIDAS Regulation

**Coverage**
19 notified eID schemes (7 mobile-based) by 14 Member States - 59% of EU-27 population has access

**Acceptance**
67% of EU-27 MS can accept notified eID schemes (node with receiving capacity). Among 7 key public services for cross-border users, only 14% offer eIDAS authentication / EU-27

**Usage**
Between 100 and 30 000 successful cross-border authentications a year compared to millions at domestic level

**User friendliness**
No common user interface, redirections in the authentication process and denial of service
Market and technological developments
Developments in the private sector and society also challenge the current status quo

**User demands and expectations**

Users want high speed, secure authentication services that protect their personal data:

- 63% want a **secure single digital ID** for all online services that gives them control over the use of their data
- 72% want to know **how their data are used** when they use social media accounts

**Private sector** organizations also want versatile, secure and trustworthy identification solutions for their users

**Role of online platforms**

Platforms are playing an important role in electronic identification.

Their market position is a challenge to **data control and user choice**.

**Technological change**

Users increasingly demand **mobile identification**

**Self-sovereign ID** is a growing trend promising to put users in control of their identity data
The European Council calls for the development of an **EU-wide framework for secure public electronic identification (e-ID)**, including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services.

*European Council Conclusions, 2 October 2020*
The Digital ID Act – Adopted 3rd June 2021
The three pillars of a European Digital Identity
The foundation of the new European digital identity

Strengthen the national eIDs system under eIDAS
Improve effectiveness and efficiency of mutual recognition of national eID schemes and make their notification mandatory for Member States.

User Controlled Digital Identity – Personal Wallet
European secure “digital wallet” trusted app on mobile/smartphone allowing the storage and use, under the sole control of the user, of identity data and various attributes/credentials, based on common standards.

Private sector as Provider of identity-linked services
Private providers to offer digital identity-linked services by following the (improved) rules applicable for qualified trust services (anchored in national eIDs).
Strengthen the national eIDs system under eIDAS
Building on the foundation established by the eIDAS Regulation

1

Security and trust
National legal eIDs will remain anchors of the new ecosystem

2

Improve supply
Provide an obligation for Member States to notify national eIDs to the Commission and therefore enable their citizens to use them in other EU countries

3

eID mutual recognition procedure
To be streamlined to reduce burden on Member States

4

Identity data
Expansion of the minimum set of identity data to be shared over the eIDAS Nodes (currently first name, family name, date of birth and gender)
User-Controlled Digital Identity – Personal Wallet

Improved user experience and use cases

1. User control
   The provision of a personal wallet:
   - Improves user-choice,
   - Improves user-experience (including mobile experiences),
   - Supports data control
   - No tracking
   - Supports portability

2. Linking Identity and Credentials
   Credentials such as driving license, university diploma, professional accreditations can be linked to the user identity.
   Users are able to manage both their identity credentials and legal eID together

3. Possible Use cases
   - Opening a bank account
   - Filing tax returns
   - Providing your age
   - Renting a car
   - Numerous digital public services
   - ...

TIP: Delete the picture and click the placeholder button to select another picture.
Possible Implementation Model for a future European Digital Identity ecosystem

**Trusted sources**
- National eID
- Tax register
- Professional Roll

**Attributes / Credentials**
- Issuance
  - Identity / Credential Provider A
  - Identity / Credential Provider B
  - Identity / Credential Provider C

**Use cases**
- Access to eGov / eHealth Applications
- Prove Professional Academic Qualification
- Access to Platforms
- Demonstrate Business Role / Interests
- Access to Financial Services
- ...
Example of the EU Digital COVID Certificate

A first use of verifiable credentials at the EU level

Definition of a minimum data set (person identification, vaccination/test information, metadata) for:

- Proof of vaccination
- Proof of recovery from COVID-19
- Proof of test result

Creation of a trust framework

- Support the verification of certificates;
- Design possible solution while complying with EU data protection legal framework and implementing its data protection principles

1. Data about the vaccination is stored in a national database (e.g. immunization registry)

2. A certificate is issued in paper or digital format and the QR code is digitally signed by the issuing authority

3. Citizen stores the certificate on the device (e.g. personal wallet)

4. Citizen presents her/his certificate to a verifier (Signature is checked in the EU public key Directory)
The European Digital Identity Wallet

Requirements

- Shall be issued by Member States (under a notified scheme) – publication of lists
- Harmonization based on standards and common technical framework, certification and conformity assessment
- Assurance level High – Security
- Sign by means of qualified electronic signatures
Onboarding of citizens to a Digital wallet (possible implementation)

1. Initiate
   - Start link your national eID with the EUeID wallet

2. Identify
   - Identity Proofing
     - Please identify with your existing eID

3. Authenticate
   - Please confirm link with your national eID

4. Use
   - Now the user may request other credentials linked to this identity and use them with service providers

The individual selects the notified eID to which they want to link their wallet.
Identity proofing to the wallet provider with an existing notified eID.
The individual is asked to authenticate (e.g., PIN code or biometrics).
Now the user may request other credentials linked to this identity and use them with service providers.
Where I can use the EU Digital Identity Wallet

1. **Online public services**

2. **Private relying parties**
   Required by law to use strong user authentication or where required by contractual obligation including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications

3. **Very large online platforms**
   *In accordance with the DSA Regulation – if requested by the user*

4. **Other service providers relying on electronic identification services**
   The Commission shall encourage and facilitate the development of self-regulatory codes of conduct
Apply for a bank loan before

1. Set up a bank appointment
2. Meeting at the bank
3. Provide all paper documents
4. Bank sends proposal
5. Set up a bank appointment again
6. Meeting at the bank again to sign the loan agreement

A document is missing
Apply for a bank loan

After

1. The user has all his documents in his personal digital wallet, from national identity to income statement.

2. He selects only the required documents asked by the bank for the loan application and sends them easily in full security.

3. The bank receives the documents electronically. If a document is missing, it is only one click away for the user. The application is ready to continue.

By using the European digital identity, this process is streamlined and more time efficient.
Private Sector as Provider of identity-linked services – electronic attestations of attributes

1. Creation of a new market
Providing a legislative framework and common standards for private and public providers of attributes, credentials and attestations (e.g., driving license, university diploma, professional accreditations ..)

2. Security and Trust
Verifiable as linked to national eID notified under eIDAS

3. Verification against authentic sources
Verification of the authenticity of attributes against authentic sources – Annex

4. Legal value
Not be denied legal effect and admissibility as evidence in legal proceedings solely on the ground that it is in electronic format
Shall have the same legal effect as lawfully issued attestations in paper format

5. Separation
Functional and structural separation of data
Additional trust services +
New eIDAS Qualified Trust Services
+ strengthening use of existing service

1. Qualified electronic archiving services

2. Electronic ledgers

3. Qualified service for the management of remote electronic signature creation devices

4. QWACS – recognition by web browsers
Unique Identification

1. Ensuring unique identification
   When the Wallet and notified means are used for authentication

2. Record matching public sector
   Where identification is required by law
Next steps
Next steps

2021

DEVELOPMENT OF ARCHITECTURE / TECHNICAL REFERENCES AND STANDARDS / IMPLEMENTING LEGISLATION

LEGISLATIVE PROCESS

TOOL BOX

2024

PILOT IMPLEMENTATION

LEGISLATIVE PROCESS

TOOL BOX