

Explanatory meeting on Chapter 32

The European Digital Identity Framework

Brussels, 19 September 2022

European Commission
DG CNECT
Unit CNECT.H4 eGovernment and Trust

These slides accompany the explanation of the acquis to Albania and North Macedonia and can only be used for that purpose. Their content is subject to further development of the acquis and interpretation by the Court of Justice of the European Union

Agenda

- The EU Digital Identity Framework and why it is important for Digital Government transformation
- The new EU regulation on cross-border use of national electronic identities

The EU Digital Identity Framework

Current legal framework

The EU Digital Identity Framework

Electronic identification

- Process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.

Trust services

- Electronic services that consist of:
 - the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
 - the creation, verification and validation of certificates for website authentication; or
 - the preservation of electronic signatures, seals or certificates related to those services;.

The EU Digital Identity Framework

Why is it important?

- Building trust in the online environment is key to economic and social development.
- Aims to provide a secure electronic interaction between citizens, business and public authorities.
- Contributes to the creation of a digital single market.

New EU Regulation on 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

The three pillars of a European Digital Identity



Strengthen the national eIDs system under eIDAS



User Controlled Digital Identity – Personal Wallet



Private sector as Provider of identity-linked services

Improve effectiveness and efficiency of mutual recognition of **national eID schemes** and make their notification mandatory for Member States

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 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) and a proposal on unique identification

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
- ...



The European Digital Identity Wallet

Main 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
- ✓ Certified
- ✓ Sign by means of qualified electronic signatures
- ✓ Free of charge



Use of the EU Digital Identity Wallet

1

Online public services

Where Member States **require electronic identification** under national law or by administrative practice to access an online service they shall also accept European Digital Identity Wallets

2

Private relying parties

Where required by law or contractual obligation to use **strong user authentication** 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

Where platforms **require users to authenticate to access online services** they shall also accept the use of European Digital Identity Wallets strictly upon voluntary request of the user and in respect of the minimum attributes necessary for the specific online service for which authentication is requested

4

All other service providers

The Commission will encourage and facilitate the usability of European Digital Identity Wallets for all other providers.

Electronic Attestation of Attributes

Private Sector as Provider of identity-linked services

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

A qualified electronic attestation of attributes issued in one Member State shall be recognized as a qualified electronic attestation of attributes in any other Member State

5

Separation

Functional and structural separation of data

Data privacy

- ✓ Full User Control
- ✓ Issuer cannot Collect Usage Data - unless necessary for wallet operation
- ✓ Issuer cannot combine identification data with personal data from other services – unless user requests
- ✓ Physical and logical separation of personal data from any other data
- ✓ Providers of qualified electronic attestation of attributes must provide such services under a separate legal entity
- ✓ Registration of relying parties
- ✓ Unique Identification
- ✓ Full application of Regulation (EC) 679/2016

Toolbox Process

Objectives

- Identify common standards and specifications (Architecture and Reference Framework – ARF) as well as guidelines and best practices

To inform

- Reference implementation of wallet
- Large-scale pilots to test wallet in national and cross-border contexts

Large-Scale Pilots (Digital Europe Programme)

Test the wallet in the context of practical use cases in national and cross-border contexts, for example:

- Mobile Driving License
- ePrescriptions
- Digital payments
- Exchange of university diplomas
- etc.

Contribute to finalising the concept of the wallet in different national contexts; identify common standards and rules for implementation

Call closing date	17 August 2022
Minimum number of participants	Entities from at least 3 Member States
Indicative budget	37 MEUR
EU funding rate (simple grants)	50%
Indicative duration of the project	24 months
Indicative start date of selected projects	By end of Q1 2023



Background documents

- **Legislative Proposal** to amend the eIDAS Regulation - [EUR-Lex - 52021PC0281 - EN - EUR-Lex \(europa.eu\)](#)
- **Recommendation on a common Union Toolbox** of a coordinated approach towards a European Digital Identity Framework - [A trusted and secure European e-ID - Recommendation | Shaping Europe's digital future \(europa.eu\)](#)
- **Press Release** outlining the Commission's proposal for a trusted and secure Digital Identity for all Europeans - [Commission proposes a trusted and secure Digital Identity \(europa.eu\)](#)
- The **Outline of the Architecture and Reference Framework** for [the reference application of] **the European Digital Identity Wallet** - <https://futurium.ec.europa.eu/en/digital-identity>
- **Call** to support the implementation of the European Digital Identity Framework - [Funding & tenders \(europa.eu\)](#)
- **Call for LSP** to [support the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation](#)

These slides accompany the explanation of the acquis to Albania and North Macedonia and can only be used for that purpose. Their content is subject to further development of the acquis and interpretation by the Court of Justice of the European Union.



Thank you

These slides accompany the explanation of the acquis to Albania and North Macedonia and can only be used for that purpose. Their content is subject to further development of the acquis and interpretation by the Court of Justice of the European Union.

Status legislative procedure

- Czech Presidency – aims for General Approach (6 December 2022)
- European Parliament – Vote in lead Committee ITRE (23 November 2022)
- Tentative date for adoption of proposal: Q3 2023