EUROSMART

The Voice of the Digital Security Industry

New European Digital Identity Framework

Summary of the European Commission's proposal

Overview of the Commission's proposal

- Date of the publication: 3 June 2021

- Legislative shape: regulation amending eIDAS as regards establishing a framework for a European Digital Identity

- Objective: transition "from the provision and use of rigid digital identities to the provision and reliance on specific attributes related to those identities"

- Means:
  -Mandatory notification of at least one eID scheme + unique & persistent identifier in the dataset
  -**European Digital Identity Wallet**, that every Member State has to put in place
  -New trust services added

Introducing a European Digital Identity Wallet

Starting point

- eIDAS has insufficient coverage
- Digital wallets on mobile devices identified as a main asset for a future-proof solution
- Private market and governments moving in this direction

Definition

European Digital Identity Wallet (EDIW)

"a product and service that allows the user to **store identity data, credentials and 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**."

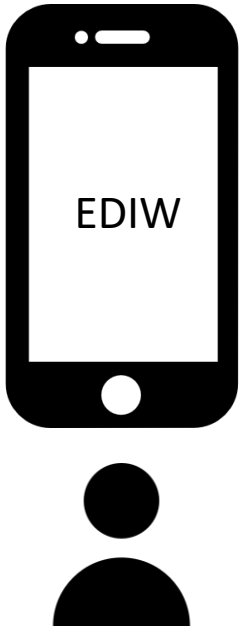
Mandatory issuance

- Member States shall issue a European Digital Identity Wallet within 12 months after entry into force of the Regulation
- EDIW can be issued under a mandate from a Member State, and independently but recognised by a Member State

→ can be provided by private parties

European Digital Identity Wallet: a common interface

Presentation of identification data and attributes in local mode (offline)



Issue qualified and non-qualified electronic attestations of attributes or other qualified and non-qualified certificate

TSP and QTSP

Relying parties

Request and validate person identification data and attestation of attributes

Note: Digital Markets Act: business users & providers of ancillary service should be able to access hardware and software features, such as **secure elements in smartphones**, and to interoperate with them through the EDIW or MS' notified eID means.

Main features of the EDIW

Security

-**security by design** (strong cryptography)

-EDIW shall be issued under a notified eID scheme level “high”

-special article on security breaches (Art. 10a)

-**mechanisms to validate attributes** provided by the Member States

Privacy

-selective disclosure of attributes

-TSP cannot receive any info on the use of the attributes

-issuer of the EDIW shall not collect info about the use of the wallet

-personal data relating to EDIW **physically and logically separate** from any other data held

EDIW can be used **cross-border** in the EU

Use is **free of charge**

New definition of eID means

“electronic identification means” means a material and/or immaterial unit, including European Digital Wallets or ID cards following Regulation 2019/1157, containing person identification data and which is used for authentication for an online or offline service

Two principles: mandatory acceptance and voluntary use of the wallet

User perspective

Using the wallet
is always voluntary

Relying party perspective

Mandatory acceptance

- Cross-border use of public services when identification using an eID is required;
- Essential services (when strong authent. required by law): transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telco;
- Very large platforms as defined by the Digital Service Act when they require users to authenticate to access online services. They shall only use the minimum attributes necessary.

Voluntary acceptance

-All other use cases;

-European Commission will encourage use with codes of conduct.

EU toolbox

- Members States should identify a Toolbox for a European Digital Identity framework.
- Toolbox will lead to a **technical architecture and a reference framework, a set of common standards and technical references**, practices and guidelines.
- **Existing international and European standards and TS** should be re-used where appropriate.
- Toolbox covers four dimensions:
  - provision and exchange of identity attributes
  - functionality and security of the EDIW
  - reliance on the EDIW including identity matching
  - governance
- Cooperation starts immediately. eIDAS expert group tasked with implementing the recommendation.

EU toolbox timeline

Sept. 2021
Launch of discussions

Dec. 2021
Agreement on technical architecture outline

June 2022
Identification of specific technical architectures, standards & references, guidelines etc.

30 Sept. 2022
Agreement between MS on the toolbox, incl. a comprehensive. architecture

30 Oct. 2022
Publication of the toolbox by Commission

Test and pilots in MS

EUROSMART
The Voice of the Digital Security Industry

Certification aspects for eID

European Digital Identity Wallet (Art. 6c)

- Mandatory certification of the EDIW with the requirements of the regulation.
- If cyber certification (CSA), EDIW presumed compliant with the cybersecurity requirements.
- Mandatory certification pursuant to GDPR by accredited public or private bodies designated by Member States.
- Commission maintains a list of certified wallets.

All eID schemes (Art. 12a)

- Voluntary certification.
- Member States may use the Cyber Act to demonstrate compliance with assurance levels.
- If certified, the eID scheme does not have to go through the peer review process.

New qualified trust service for attestation of attributes

New qualified trust service

- Purpose: Attestation of attributes relating to identity
- Requirements for qualified electronic attestation of attributes (Annex V)
- Providers of qualified electronic attestations of attributes provide an interface with the EDIW
- Attributes can be verified by the QTSP or via a designated intermediary

Minimum list of attributes (Annex VI) that MS must allow QP to verify against authentic source at national level:

→ address, age, gender, civil status, family composition, nationality, educational qualifications, professional qualifications, public permits & licences, financial & company data

Privacy safeguards

Providers of qualified electronic attestation of attributes' services shall provide such services under a **separate legal entity**

Identity proofing in the context of QTS

QTSP must verify identity when issuing a qualified certificate or qualified electronic attestation of attributes. They can rely on:

- eIDs levels substantial or high
- qualified electronic attestation of attribute or a certificate of a qualified electronic signature/seal (relying itself on another type of identity evidence)
- other identification methods offering a high level of confidence
- the physical presence of the natural person or a representative of the legal person

Other new trust services

- Electronic archiving
- Management of remote electronic signature and seal creation devices
- Electronic ledgers

Trust services: international equivalence

Commission can decide that TSP established in a **third country are subject to requirements equivalent to the requirements applicable to QTSP** established in the EU.

→ Commission adopts an implementing act or concludes an international agreement on mutual recognition of trust services

→ TSP established in that third country shall be considered equivalent to QTSP established in the EU

→ those TSP can use the EU trust mark for QTS

Trust services: security

NIS 2

- Full alignment with NIS 2: trust services considered essential entities in NIS 2 so must comply with all the NIS 2 requirements
- eIDAS updated to take into account this change (references to NIS 2 added)

Obligation for QTSP

- Appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible

Trust services: standardisation

The Commission will reference standards and technical specifications…

… within 12 months after entry into force for:

- conformity assessment schemes for carrying out the conformity assessment of the QTSP by the CAB
- requirements for QTS
- verification of identity and attributes by QTSP, including identification methods offering a high level of confidence
- qualified certificates for electronic signature
- etc.

…within 6 months after entry into force for:

- qualified electronic attestations of attributes in the context of the EDIW
- catalogues of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes in the context of the EDIW