



European Digital Identity Framework

A photograph of the European Union flag, which is blue with twelve gold stars arranged in a circle. The flag is being held up by two hands, and it is waving in the wind. The background is a blurred green landscape with trees.

Anders Gjøen,
European Commission, DG CONNECT
eGovernment and Trust

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

Very few 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

*Report on the evaluation of the eIDAS Regulation

Market and technological developments - **evolution**

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

Mobile identification and user-controlled identity systems are increasingly in demand

Emerging needs and requirements in the market

Provision and reliance on specific attributes related to identities.

Focus on both the private and the public sector use cases

The three pillars of a European Digital Identity Framework

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**, e.g. by optional certification, and make their notification mandatory for Member States



User Controlled Digital Identity – Personal Wallet

European secure trusted “digital wallet” app on mobile/smartphone allowing the storage and use of identity data and various attributes/credentials, based on common standards, under the sole control of the user,

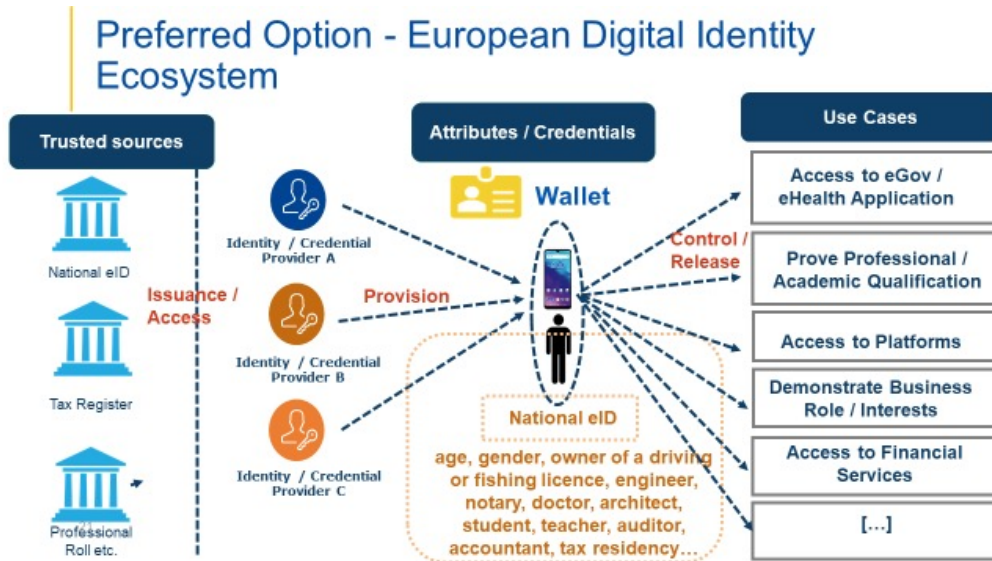


Private sector as Provider of identity-linked services

Private providers to offer **digital identity-linked services** by providing (qualified) attestations of attributes to the wallet following the (improved) rules applicable for qualified trust services (anchored in national eIDs).

Commission proposal 3 June 2021 (COM (2021) 281)

Harmonization and introduction of a wallet



- A harmonized requirement is introduced at level high
- Under a notified scheme
- The MS states will be obliged to issue it to all citizens and residents free of charge – role of private sector
- Harmonization by adherence to common standards and certification*
- Deadline of 12 months after coming into effect

*Commission Recommendation of 3.6.2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework + implementing acts

The European Digital identity Wallet

The user perspective

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 to Attributes and Credentials

- *Credentials such as driving license, university diploma, professional accreditations can be linked to the user identity and issued to the Wallet*
- *Users are able to manage both their identity credentials and legal eID together*

3

Use Cases

- *Authentication,*
- *Electronic signature,*
- *Opening a bank account,*
- *Filing tax returns,*
- *Proving your age*
- *Renting a car*
- *Numerous digital public services*

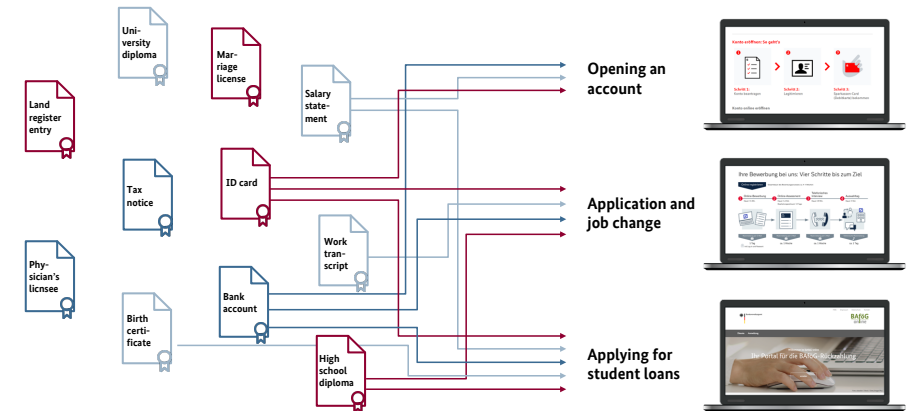
Required acceptance – 12 b

- Public services and a broad range of private services will be **required to accept authentication with this mean.**
 - Transport
 - Energy
 - Banking and financial services
 - Social security
 - Health
 - Drinking water
 - Postal services
 - Digital infrastructure,
 - Education
 - Telecommunications
- Where very large online platforms as defined in the DSA Regulation Article 25.1. require users to authenticate to access online services, they shall also accept the use of European Digital Identity Wallets
- Codes of conduct – ensure acceptance
- Review clause



Introduction of attested attributes

- Qualified Trust Service
- Legal effect – 45 a
 - Not denied legal effect
 - Same legal effect as lawfully issued attestations in paper forma
 - Qualified electronic attestations of attributes to be recognized as a qualified electronic attestation of attributes in any other Member State
- Electronic attestations of attributes in public services – 45b
- Verified against authentic sources – 45d
- Data protection requirements – 45 f
 - Functional separation
 - Physical separation



Other proposed changes

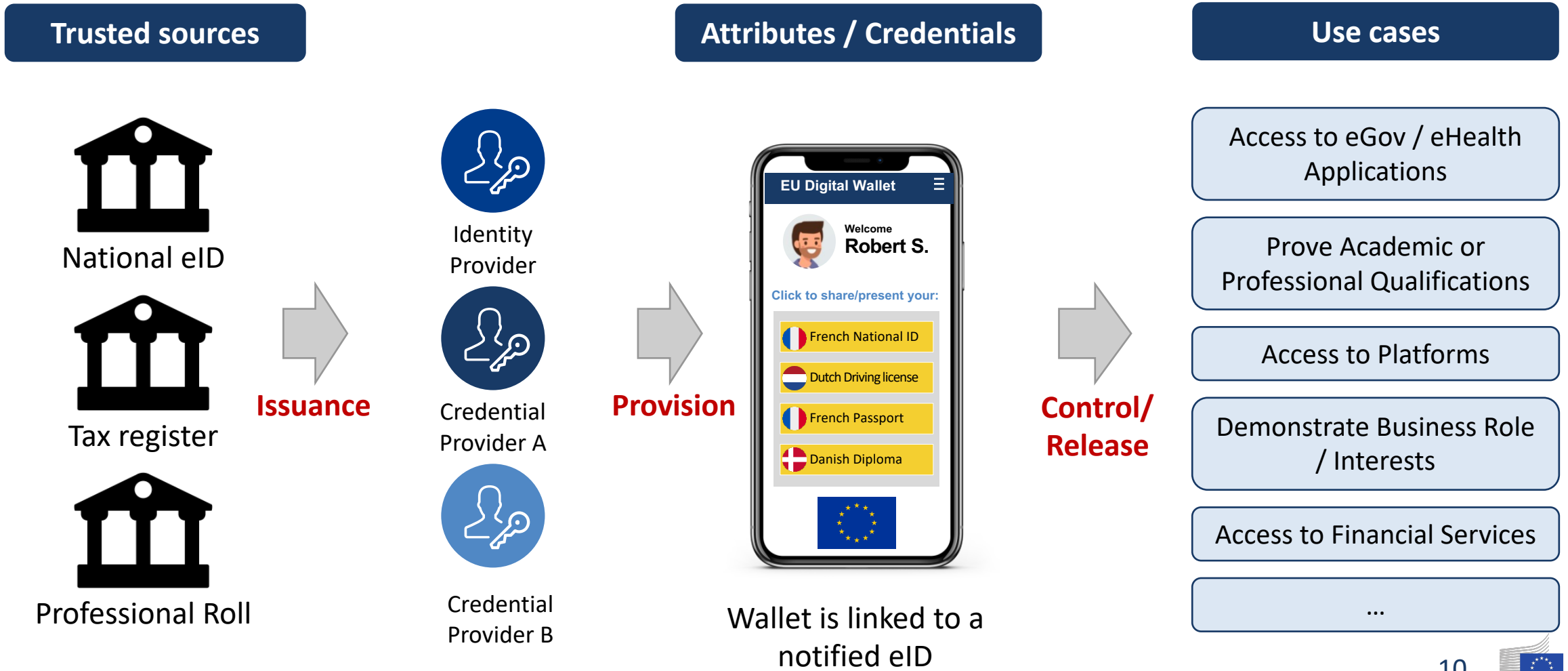
European Digital Identity Wallets

- **European Digital Identity Wallets Relying Parties – Article 6b**
- **Wallet - Identity matching – Article 11a**
 - Introduction of a unique persistent identifier
 - Requirements on identity linking for the MS
 - Goal to facilitate access x-border to entitled public services

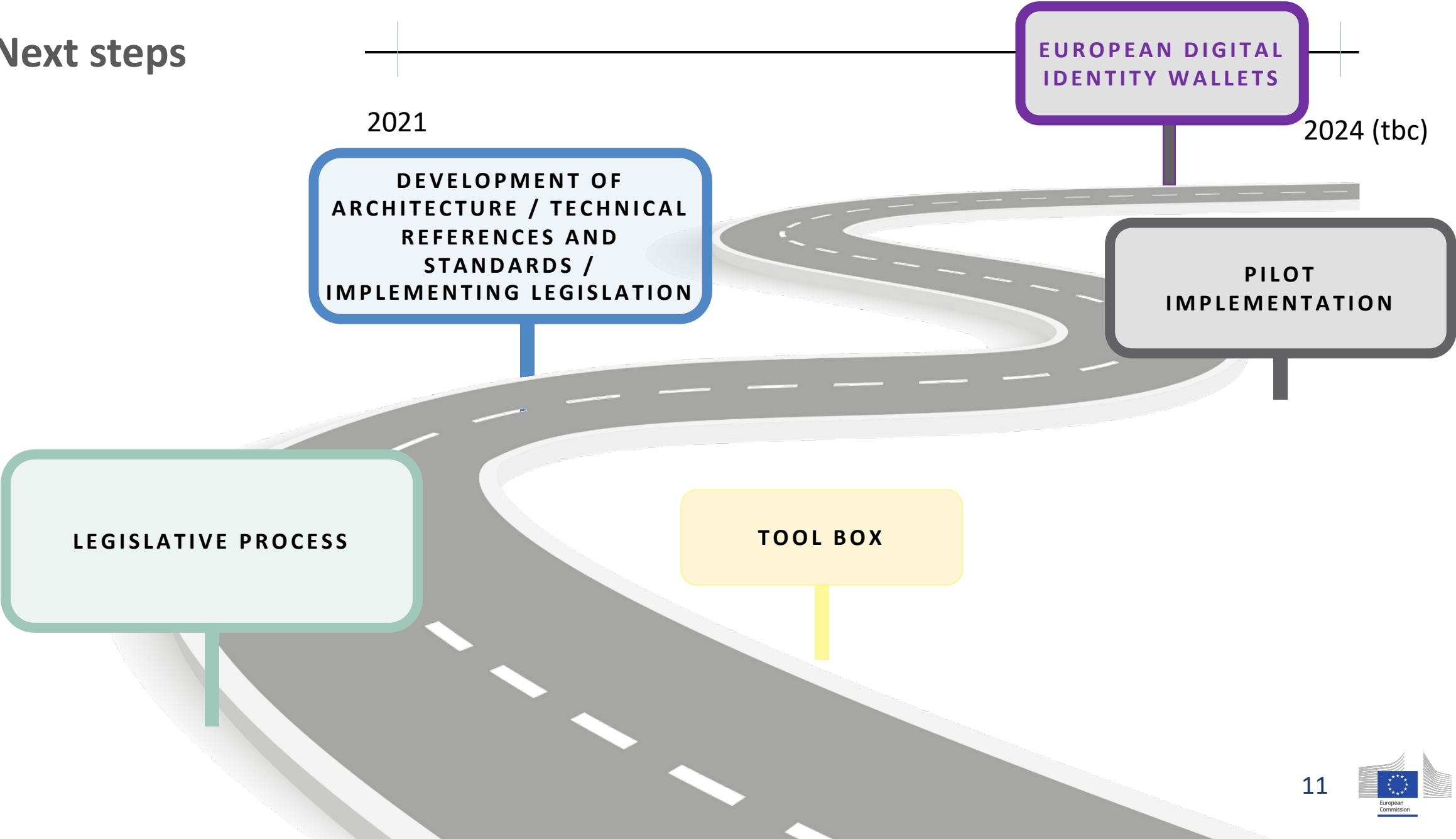
Trust Services

- **Qualified service for the management of remote electronic signature creation devices – 29a**
- **Qualified electronic archiving services – Article 45h**
- **Qualified Electronic Ledger – section 11**
 - Requirements for qualified electronic ledgers
 - Recognition on the usage of electronic ledgers for non-repudiation and sequencing
- **Qualified Web Authentication Certificates – section 10**
 - Browsers - requirements for support and acceptance

The future European Digital Identity ecosystem



Next steps



Thank you

[European Digital Identity | European Commission \(europa.eu\)](https://european-digital-identity.ec.europa.eu/)



© European Union 2020

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

Slide xx: element concerned, source: e.g. Fotolia.com; Slide xx: element concerned, source: e.g. iStock.com