IDEMIA

9 facts about the EU Digital Identity Wallet

# IDENTITY

POSTED ON 10.30.23

The EU Digital Identity Wallet is an ambitious digital identity project launched by the European Commission with the aim of boosting the single market and creating EU champions by streamlining cross-border identity verification. Pilots have been launched both to test the infrastructure and work on the EUDI Wallet's technical features alongside its legal aspects—a rather unusual process, but one that should speed things up. The regulation should be approved by the end of 2023, along with the implementation timeline—the EU Digital Identity Wallet should be available within the next 2 to 3 years.

The EU Digital Identity Wallet aims to streamline and **secure a wide range of eGovernment services** for EU citizens such as requesting birth certificates, medical certificates, reporting a change of address or filing tax returns. **It should also benefit the private sector** whenever identity verification is required—opening a bank account, renting a car, checking into a hotel, etc.

- How will this digital ID wallet co-exist with existing ID documents and national digital identity systems?
- Who will issue the EU Digital Identity Wallet?
- Can we trust the EU wallet to protect our identities and respect our privacy?

Read on to get some answers as well as a better understanding of the EU Digital Identity Wallet.

1. The EU Digital Identity Wallet will be available for every citizen throughout the EU

Today, only 60% of the EU population in 14 Member States are able to use their national eID across borders[1]. **The new version of the eIDAS** (Electronic IDentification Authentication and trust Services) regulation, will make the EU Digital Identity Wallet available to any EU citizen, resident, or business who wishes to use it. Unlike eIDAS I, which introduced a preliminary framework for digital identity deployment and usage in the EU, **the eIDAS II regulation will mandate EUDI wallet implementation for all member states**, with a strong focus on interoperability. The eIDAS II regulation will also provide access to private sector players. The aim is that by 2025/2026, every European citizen will have access to a digital identity compliant with EU standards and accepted by authorities and service providers across all member states.

2. The EU Digital Identity Wallet is NOT going to replace existing ID documents

The EU Digital Identity Wallet will provide a digital version of ID documents and other personal documents: identity cards, driving license, passports, payment cards, transport cards, travel passes, etc. One of the main advantages of the

EU Wallet is that it will **facilitate online identity verification**. Because it will be standardized at the EU level and recognized by all member states, the EU Digital Identity Wallet will open up new cross-border use cases such as opening a bank account, applying for a university or filling in a medical prescription in another member state. It will also allow EU citizens to **travel throughout Europe without their physical ID documents**. Border control authorities will only need a smartphone or tablet with a specific application to check the wallet holder's identity.

However, for the present, the EU Digital Identity Wallet is intended to complement rather than totally replace existing physical ID documents. Both will have the same use and value. **Physical and digital ID documents will coexist**, not only because the smartphone containing the EUDI wallet can always break down or run out of battery, but also because the physical ID document should still play **a key role in securing the EU Digital Identity Wallet** in most countries—but more on that later.

3. The EU Digital Identity Wallet will be implemented at national level

The regulations and technical standards will come from Brussels but implementation will take place at national level. There is no EU wallet just yet, but **certain Member States have already developed digital identity apps** with similar features, including France, Portugal and Austria, although they are not interoperable just yet. The objective is to make these national apps evolve to integrate eIDAS protocols and standards.

4. All EU Digital Identity Wallets must be interoperable, but their features may vary

While the European standard will define interoperability at national level for the EU Digital Identity Wallet, each member state will be free to implement it however they wish. This means that **each member state will be able to use its own designs and features**, but that every EU wallet will share certain common features and be interoperable across the EU. In addition to compliance with **EU interoperability standards**, EUDI wallets will also have to obtain **security certifications implemented at national level**.

5. The EU Digital Identity Wallet may be developed by the government or by a private sector provider

Member states may create the wallet by themselves or **commission a private-sector provider** (most likely from the banking, telecoms or utilities sector). However, these private players will not be allowed to monetize the wallet, which must remain free of charge for all citizens.

Different approaches exist within current working groups. France uses framework agreements with the private sector while Belgium relies on a consortium of banks and mobile network operators. In any case, while the EU Digital Identity Wallet will primarily be a **public-sector initiative**, the private sector will be involved to a greater or lesser extent. And, unlike its first version, eIDAS II will place a strong emphasis on private sector use. All service providers and major platforms will have an **obligation to accept the wallet** for identity verification—especially in regulated sectors such as finance and telecoms.

6. The EU Digital Identity Wallet will be highly secure

As a **native digital solution**, the EU Digital Identity Wallet will be more effectively adapted to – and help to prevent fraud in – remote and digital inspection. Authentication checks will be quick and easy—users will simply have to scan a QR code, tap a PIN code and/or hold their eID card up to their smartphone.

The new European regulation should define **two levels of security** for EU wallets: **a high and a substantial level of security**. Each country will be required to have at least one high-level security wallet. However, other wallets may be created within the same country either by private or other public actors. Whether these additional EU digital identity wallets implement a substantial or high level of security **will depend on the use cases**. For instance, a Health Ministry could implement a separate EUDI wallet to provide specific features that streamline patient care and such a wallet is likely to require a high level of security. Other wallets providing slightly lower—but still "substantial"—levels of security while **offering greater ease of use may be considered for less demanding use cases**.

7. A secure element will be used to secure the data

The level of security (high or substantial) will depend directly on the **certification of the secure element** hosting the keys of the EU Digital Identity Wallet. These keys will prevent unauthorized access to sensitive personal data using encryption. Ideally, this would be based on an existing secure element embedded in a smartphone but there is no guarantee that all smartphones will be compatible. This could also pose problems of sovereignty if phone manufacturers retain control of the technology and are in position to prevent governments from gaining access at some point. Hence the current discussions between Big Tech and the European Union.

The easiest way of solving these sovereignty and security certification challenges at present is to **use the secure element already embedded in national eID cards**—as is the case in France. The ID card chip is issued by the government and therefore poses no problems in terms of sovereignty or security. The wallet holder will need an NFC-enabled smartphone to unlock the wallet using their eID card and share any sensitive personal data.

For member states preferring to **use a secure element already embedded in the phone for better ergonomics**, another alternative could be to use the SIM card. In any case, the EU Digital Identity Wallet security level will only be considered high if the secure element is certified by the government and guarantees sovereignty over the EUDI wallet keys. If the smartphone-embedded secure element or the SIM card are not certified, they may still be used for less critical, more ergonomic EU wallet applications.

8. The wallet will protect personal data

Ultimately, the EU Digital Identity Wallet **will provide enhanced privacy** and safety for citizens and consumers who need to confirm their identity **either online or in-person**. The user may share only those ID attributes and personal data that are relevant for a specific transaction—no copies can be made without the user's knowledge.

In concrete terms, the user will receive a validation request on their smartphone to share the attribute requested. **No more paper copies** of ID documents at hotel check-in desks or car rental companies, **no more electronic receipts** of ID cards, passports or driver's licenses sent by email. For example, wallet users will be able to prove the validity of their driver's license without displaying their address. In terms of privacy protection, they may even be able to access services reserved for adults without revealing their identity—if permitted by national regulations.

Moreover, there will be **no centralized data system**. Each citizen's EUDI wallet will store their personal data—attacks against EU Digital Identity Wallets will not be scalable.

9. Using pseudonyms rather than unique identifiers will avoid cross-linking databases

A unique identifier is a single number associated with one individual and cannot be changed during the user's lifetime. Creating different pseudonyms **sector-based or even service-based** (for banking, healthcare, insurance, etc.) is a way of preventing that number from being used for cross-linking databases and tracking users. The European regulation should allow each Member country to assess whether using a unique identifier is a concern at national level or not. It should also allow for more flexibility and greater privacy protection through the use of pseudonyms that may even change over time. In any case, a unique identifier or pseudonym **must remain independent of the digital ID wallet** as users will need to keep these codes in case they need to change their phone and reinstall their wallet on the new phone.

As regards the numbers to be used for the unique identifier or pseudonyms, this is also **likely to differ from country to country**. Italy could use people's tax ID as a unique identifier while France or the Netherlands would likely prefer to have sector-based pseudonyms, such as social security numbers in France for health-related matters.

[1] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en