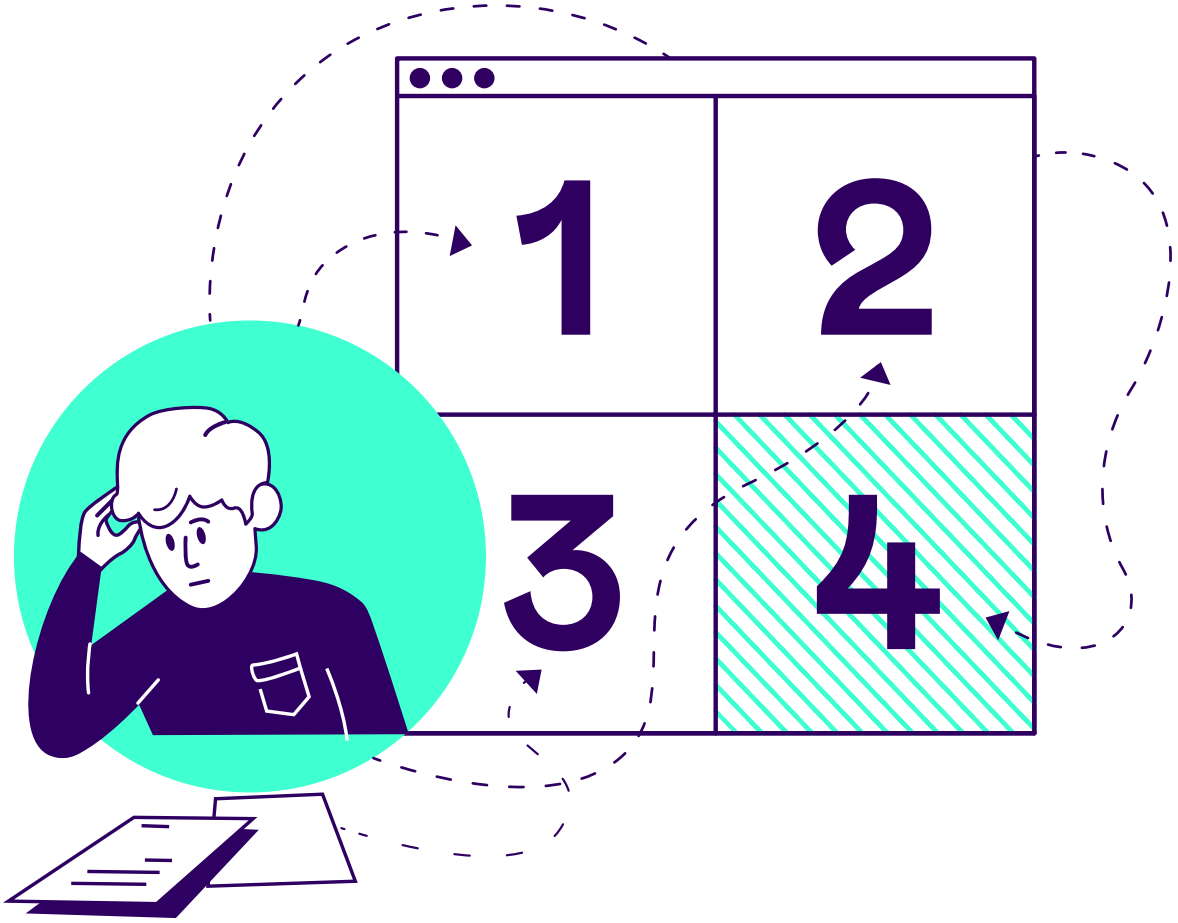
Signicat

4 ways the EU Digital Identity Wallet could fail



When it comes the European Digital Identity Wallet – also known as the EU Wallet – we all agree that it will be great, but we don't really know what it will be. In this post, we discuss some of the unknowns and why, if these are not addressed, the Wallet could fail.

What is the European Digital Identity Wallet?

The EU Wallet, formally called the European Digital Identity Wallet ("the Wallet") is an initiative by the European Commission to provide electronic identification and other identity-related functionality to all citizens and residents of EU Member States, including the EEA countries, Norway, Iceland, and Liechtenstein.

The Wallet will be regulated in a revised version of the eIDAS ("eIDAS 2.0") regulation (Regulation (EU) 910/2014). Their goal is to provide electronic identification and trust services for electronic transactions in the internal market (the EU). This regulation is accompanied by the European Identity framework act. Both eIDAS 2.0 and the framework are a work in progress, meaning we do not yet know exactly what the Wallet will be.

The concept of the Wallet was launched by Commission President, Ursula von der Leyen, in her State of the Union address in September 2020. In February 2022, the Commission put €37m (50% of the total funding) on the table for large-scale pilots to identify what infrastructure would be needed to establish the Wallet. In total, €74m has been made available for at least four pilots over a two-year period from early 2023. An additional €26m was commissioned in June 2022 for provisioning of a reference application for the development of the Wallet.

The Commission shows a determination to make the Wallet a success, but is success the guaranteed outcome? In our view, certainly not! Not that we expect the initiative to fail, and by no means do we want to see it fail, but there are certain risks that don't currently seem to be taken into consideration.

4 potential risks of the EU Digital Wallet

Below, we outline what we see as the main risks that may affect the success of the Wallet. Note, in this post, we're not attempting to quantify the risks or necessarily propose mitigating measures.

The risks are described by conditions that might cause them to materialise. Mitigation of these risks should be included in the scope of the large-scale pilots and the work of the eIDAS Expert Group of the Commission, and they should be considered as part of the work to finalise eIDAS 2.0.

The four risks are:

1. Lack of buy-in from key parties and EU citizens
2. A Wallet ecosystem that is not commercially sustainable
3. Technical immaturity and an over complex solution
4. Legal incompatibility with existing regulations

1

Lack of buy-in from key parties and EU citizens

Will we trust the Wallet?

According to eIDAS, the government will be responsible for issuing the Wallet. This means that the Wallet will either be issued by national government, on behalf of government, or by private sector actors approved by government.

The Wallet as a government responsibility may be a source of trust for some Member States and some groups of the population, and not so much to others.

People are used to getting their identity documents from the government, but when it comes to digital data people respond differently. There must be trust that the government does not spy on the Wallet holders or otherwise abuse the Wallet and what it may contain. Some concerns about this have already been voiced, describing the new reform as 'Orwell's wallet'.

Since the Wallet will potentially hold a lot of personal data, it is not only important that the Wallet is secure, but also that it is perceived as secure by the citizens using it. Users will want reassurance that the personal information in the Wallet will be safe, and that the issuer won't abuse this information.

If the Wallet isn't secure, it will be distrusted and for good reason, but even a secure Wallet can be harmed by just the perceived lack of security.

Insufficient user demand for the Wallet

The Wallet will be a voluntary offering to EU citizens, but users will only buy into it if they find it useful. This is a potential deadlock for any electronic ID (eID) deployment:

- Users are only interested if the services it offers are of value to them
- Service providers are only interested if there is a sufficiently high number of users are using that service frequently enough.

The Wallet will fail unless the user experience is valued by the users, meaning that it must exceed that of other eID services in the market. One key aspect of this is ensuring that users have sole control of their Wallet, but that they're not left to themselves if problems occur, i.e. if their Wallet is compromised or lost, or the device holding the wallet is lost.

Not enough deployment efforts by Member States

eIDAS 2.0 will impose an obligation on all EU Member States to ensure a national Wallet offering. While no Member State has objected to this obligation, some Member States may not prioritise this task, by establishing only a nominal Wallet offering to formally fulfil the obligation.

When a Wallet is issued by or on behalf of a Member State, the government of that nation can play a key role in ensuring its deployment in society, facilitating usage by its citizens and service providers. But deployment does not happen by itself, and governments are not necessarily the best experts in sales and marketing.

Lack of government service provider buy-in

Government services will be required to accept the Wallet; this includes any Wallet issued in another Member State. This mimics the current eIDAS requirement that government services are obliged to accept eIDs notified by other Member States, though few government services actually comply with this requirement today.

Accepting foreign Wallets may be easier since these should adhere to the same specifications as the Member State's own national Wallet(s). But a basic problem remains: How can a governmental service provider use a foreign identity?

Today, government services are designed to serve citizens and residents of their own country, according to the rules of their own government. The identification provided by a foreign eID, and soon by a foreign Wallet, may not work without access to national data. And mapping a foreign person to the corresponding national identity, if that identity exists, is very difficult.

EIDAS 2.0 suggests adding a persistent unique identifier to the identification provided by a notified eID or Wallet. While this may simplify the cross-border linking of identities, the proposal is highly controversial in Member States that today restrict the usage of unique national identity numbers.

The result may be that government service providers will continue to cater for their own residents while ignoring users from other Member States.

Not fully catering for private sector needs

Getting private sector service providers actively engaged in the Wallet project is core to making it a success. While government services are important, experience shows that such services alone are not enough to obtain sufficient value to the users. But the needs of the private sector are different from those of the government.

For most of their online transactions, private services need contact details (phone, e-mail, address) and support for payments, where governments focus on identification and authentication. Wallets not only need to cater for private sector needs, but to support them in ways that are efficient and user-friendly.

Almost all successful eIDs deployments are public-private sector collaborations involving governments, banks and other financial service providers. The financial sector involvement is crucial because these services are used frequently and require high levels of security, so they also build trust towards such services in society.

Private sector service providers will be obliged to accept Wallets issued in any Member State under eIDAS 2.0. These could include regulated industries, but also large platform services. There is a possibility that service providers either ignore this requirement or that they only nominally fulfil it, i.e. making it available for use but with no promotion or even actively discouraging its use to favour other methods.

2

A wallet ecosystem that is not commercially sustainable

Exclusion of key business models within the Wallet ecosystem

For the Wallet to become a valuable asset in a user's everyday digital life, an ecosystem is needed to provide the full functionality of all sorts of transactions. The Wallet will be supported by a whole set of services, such as creating electronic signatures, issuing and validating attestations, referencing trust lists and more.

This ecosystem is described in the first version of an Architecture and Reference Model (ARF), published by the Commission. The ARF presents about 10 different provider roles that would make up the Wallet ecosystem. This will never be realised unless all roles have a sound business model. There are two alternatives:

- A role must be commercially viable, meaning the actors get paid
- A role must be funded by government.

The business models are not part of the ARF or eIDAS 2.0 and some key requirements are missing. Importantly, the issuer of identity data cannot know if or when their data is being used in a transaction with others, and the user cannot be charged for the Wallet or the identity data.

The same applies when using an authentication service or attribute attestation provider. So, with no communication between the service provider and the attribute attestation provider permitted, setting up a payment scheme could be costly given the security and compliance requirements. The actor would need to have confidence in the number of transactions paid for through the service.

There is another aspect of this business case: will the service income cover the cost, or will we face only governmental attribute issuers?

Identity providers unsure how to respond

There are currently many private sector initiatives deploying wallets with lots of innovative approaches that can support many new use cases. This is a relatively new development and most of the private sector actors are eagerly looking for opportunities. Currently, the Wallet seems to cause confusion to the actors of the identity services industry since providers are unsure how to respond.

Wallets will be issued nationally by government, on behalf of government, or by private providers approved by government in eIDAS 2.0. The opening for the identity service provider industry will be limited to the 'government approved' alternative.

Presumably, many Member States will choose to issue Wallets themselves, with some choosing commercial providers, but there is no guarantee that market access given in one Member State will extend to another.

Given the potential complexity and cost of operating a wallet service, this situation may be too uncertain and restricted for commercial actors to take the risk.

Knowing that there will be limited opportunity to deploy their wallets on a larger scale without securing broader Member State sponsorship, this might stop the current innovations and developments for a longer period.

The reference implementation that will be developed by EU funding will still exist. How the Wallet is used may also be restricted. Some governments would like to limit access to the identity or data perceived to be sensitive in the Wallet to public sector and specific regulated industries.

There are worries about commercial abuse of personal data, something that could be mitigated by forcing service providers to be registered to be able to use the Wallet. This might lead to private sector actors developing other wallet services as an alternative to the Wallet.

The best way to deploy the Wallet would be to define its issuing as a qualified trust service. This would make it a well-regulated, audited and supervised commercial service in the internal market.

Member States would still be in control of national identity, through issuing identity cards, passports and other identity documents. In addition, national identity should include a government-based eID, e.g. an eID stored in the chip on national identity cards.

3

Technical immaturity and an over complex solution

Too complex to realise in a short timeframe

Is the EU Commission underestimating the complexity of the Wallet project and the technology needed to make the Wallet and its infrastructure a reality?

The required functionality from the current proposal for eIDAS 2.0 and its timeline - all Member States issuing the Wallets within 12 months after entry in to force of the revised eIDAS – are very ambitious. eIDAS 2.0 is expected to enter into force in early 2023 meaning the Wallet could be issued in early 2024.

The technology is not ready

The technology and standards (see below) needed for the Wallet are fresh off the drawing table, or not even finished yet. There are only a few production-level implementations in place, such as W3C verifiable credentials, but none of them are being developed at a large scale and most of them are still being worked on.

Getting the Wallet to work with such a wide variety of standards to choose from will be the least of the concerns if you think about the need for interoperability: how many protocols does a service need to support? What about users needing to transfer to another wallet?

Lack of standardisation bodies and too many standards

The EU formally recognises only a limited number of standardisation bodies, or European Standards Organizations (ESOs). In Europe, this includes ETSI, CEN and CENELEC, and internationally ISO and ITU.

Many other bodies publish openly available specifications, or 'standards', such as IETF and W3C. Such specifications as a rule cannot be referenced at EU or Member State level. An approach used for eIDAS trust services is that ETSI or CEN produce EU-referenceable standards based on such specifications. This work takes time as discussed below.

Many specifications exist in the Wallet ecosystem but few are classed as formal standards. For example, about eight different specifications have been identified as a possible basis for attribute attestations, but many of these are not compatible with each another.

A decision must be made on whether there will be strict adherence to formal standards or not. Strict adherence may be desired but it will exclude many specifications that can provide a good approach for the Wallet ecosystem implementation.

Short-circuiting standardisation processes

In ETSI, a Specialist Task Force (STF) is put together to produce technical standards. Embedding such standards into EU standardisation bodies is a long and complicated process and can take at least 1.5 years. With a European Norm (technical standards drafted and maintained by ESOs) the timeframe can be longer due to an approval process with the Member States.

While work has started on supporting the Wallet, it is unlikely that the standards will be ready for deployment in early 2024 as proposed.

To deliver a Wallet reference implementation, the Commission has asked the selected vendor to deliver a first implementation of the Wallet within four months from start of the project.

This effectively means that vendor would have to begin the project in advance of this date, using technology selected by them. This may result in the vendor setting the technical scope and standards for the Wallet.

Lack of interoperability with other eID schemes

From the eIDAS 2.0 proposal, you might get the impression that the Wallet will be the only eID service in the EU. This won't be the case. The eIDs that are deployed in many Member States today will continue to exist for quite some time. Service providers will face challenges supporting several eIDs, including the Wallet, for their services.

The ARF recognises this situation by allowing an 'authentication gateway', or broker, as an intermediary between the Wallet and relying parties or governmental infrastructures.

This means that an actor, such as Signicat, can integrate the Wallet as one more eID service into the broker alongside other eIDs and offer access to all of them through one API.

---

4 Legal incompatibility with existing regulations

Incompatibility with GDPR

The European data protection regulation, GDPR, (Regulation (EU) 2016/679) establishes the roles of data controller and data processor for actors holding personal data.

It's not clear how these roles, and GDPR in general, can be applied to the case of the Wallet. When I download personal information to my Wallet and disclose this to a relying party under my sole control, am I my own data controller? Can I authorise the relying party as a data processor? Who is liable if the said data processor makes a mistake? And to who are they liable?

Privacy and data protection is vital for both GDPR and the Wallet. There should be no conflict between them but their relationship must be clarified.

Incompatibility with the Single Digital Gateway regulation

The Single Digital Gateway Regulation (Regulation (EU) 2018/1724) requires Member States to establish a network of national portals to provide information for citizens and businesses.

The regulation is based on the 'once only principle', which implies that "citizens and businesses will provide their data only once to public administrations", and "competent authorities from a Member State will be able to send your data in real time to their counterparts in other Member States".

An infrastructure is being established to support the Single Digital Gateway regulation, where a person can authorise the release of their information to a counterpart, and the information will then be delivered over this infrastructure.

An important aspect of the single digital gateway is the ability to search for information, which may fit well with the concept of the Wallet, and also be useful for the user. However, the Wallet and the single digital gateway infrastructure seem to provide two parallel but incompatible mechanisms for exchange of attributes; one through the Wallet under sole control by the user, the other through the single digital gateway infrastructure authorised by the user.

The information sources for the single digital gateway infrastructure can be the same as the 'authoritative sources' for the attributes in the Wallet. The Single Digital Gateway and eIDAS are two EU regulations aiming to solve similar problems but in two different ways, and the legal situation needs to be clarified. If two infrastructures are being built for partly overlapping purposes, it would be a waste of EU and Member State budget.

Potential breech of EU fair competition and government subsidy regulations

If a Wallet issued by or on behalf of government is introduced in a Member State where an infrastructure of commercial eID providers exists, the government will become an actor in the eID market.

A government can issue a subsidised or free eID for access to public services, but when the eID is offered to the private sector as the Wallet will be, the government may end up competing with commercial actors, and EU regulations on fair competition and state subsidies may come into play. This legal challenge is linked to defining business models for actors in the Wallet ecosystem.

Lack of alignment to existing payment schemes

Use of the Wallet for payments is not mentioned in eIDAS 2.0 but it has emerged as an important use case for the large-scale pilots.

It is still unclear what the payment functionality of the Wallet will be; will the Wallet merely provide Strong Customer Authentication (SCA) to support a payment transaction, as defined by the PSD2 Directive, or should the Wallet offer its own functionality for payment transactions?

Regardless of how this will work, it's important that the Wallet is aligned with existing payments schemes as the payment industry has its own set of agreements and regulations, which need to be complied with.

Ideally, SCA should be a requirement of the Wallet. However, if a payment service is provided by the government in competition with commercial payment service providers, this could also be affected by EU fair competition and state subsidies regulations.

To summarise, there are many reasons why the European Digital Identity Wallet initiative could fail. This blog post has highlighted the risks grouped into four categories:

1. Lack of buy-in from key parties and EU citizens
2. A Wallet ecosystem that is not commercially sustainable
3. Technical immaturity and an over complex solution
4. Legal incompatibility with existing regulations

So why does Signicat believe that the Wallet may still be a success? While that is a topic for another blog post, the short version is that the Wallet initiative has caused a revival of the identity services industry.

It highlights the aspects of sole user control and targeted identity, meaning the user is in control of releasing only the specific information that the receiver needs. Many, if not most, identity experts believe that this is in principle the way to build identity services, but the idea appeared to be parked in the research labs. Now it might happen in real life. Or actually it will happen, because even if the Wallet should fail other similar services will appear.

Signicat is involved in the developments and pilots that try to bring this new Wallet ecosystem to life. Being aware of all the risks involved, we know this may not result in the all-encompassing great shiny single solution some people envisage. But it will be a major step ahead in facilitating the needs for real trust in the digital world.

About Signicat

Signicat is a pioneering, pan-European digital identity company with an unrivalled track record in the world's most advanced digital identity markets. Its Digital Identity Platform incorporates the most extensive suite of identity verification and authentication systems in the world, all accessible through a single integration point.

The platform supports the full identity journey, from recognition and on-boarding, through login and consent, to making business agreements which stand the test of time. Signicat was founded in 2007 and is headquartered in Trondheim, Norway.

Contact us