Partnership for
Cyber Security
Innovation

Position paper

The eIDAS2 legislation will benefit from a broader technical and functional perspective

The purpose of this document is to provide a commentary on current discussions around the new eIDAS amendment. This amendment implements the current Commission's vision, which is summarised by the Commission's president as follows:

> *"Every time an app or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will propose a secure European e-identity. […] A technology where we can control ourselves what data is used and how."*
>
> Ursula von der Leyen, 16 September 2020

The intended new legislation

The European Commission is working on a proposal for a secure European Digital Identity Wallet (EDIW), amending Regulation (EU) No 910/2014.

The introduction of the EDIW will have great benefits for individuals and businesses in Europe. To name a few: it will open up the currently localised market for digital services in the EU, and it will enable individuals to interact fully digitally with organisations, replacing the current hybrid form where information with high assurances has to be supported with physical evidence (passports, qualifications, etc.). Furthermore, institutions will receive verified information about their customers, which will enable them to further digitalise processes, saving on operational costs and improving customer satisfaction. However, despite the obvious benefits, the introduction of the EDIW also raises some concerns.

Concerns

The amendment will require legislation in all Member States to at least notify one EDIW. All major institutions in specifically mentioned industries, such as the healthcare sector and financial industry, will then be required to accept these notified EDIWs. Our concern is twofold:

1. Loss of control due to forced acceptance of third-party identity wallets, as these will open up security risks that have so far been covered using proprietary solutions[1]
2. The risk that the regulation focusses on a single technological solution that excludes specific use-cases. [2].

1. Loss of control due to forced acceptance of third-party identity wallets

Currently, companies control customer identification and the associated security because they control the apps, proprietary or otherwise, being used. Most apps perform client-side detection of irregular behaviour or account takeover. If companies are required to use a plethora of notified third-party EDIWs, they will also be forced to make do with the security features of those identity wallets, which are

[1] In-depth Article - Loss of Control due to EDIW
[2] In-depth Article - More versatile EDIW

not guaranteed to match their risk profile. This risk has also been described in the third revision of eIDAS2. This PCSI proposal aims to continue enabling client-side detection for verifying companies and retain a predefined level of control to mitigate risks of fraud.

This can be achieved by taking three measures[3]:

1. **Verifying the App.**
   The proposal should enable the verification of apps for specific use in industries and enable industries to accept only those apps that accord with their specific risk profile.
2. **Device binding.**
   The proposal should enable companies to introduce methodologies that ensure they are still communicating with the originally onboarded device.
3. **Right to refuse.**
   In the event that the verifier notices irregular behaviour or changes based on the previous two measures, it should be allowed to temporarily reject any client EDIW deemed unsafe and, in case of structural problems, the unsafe EDIW as a whole. In the eIDAS2 proposal, this is addressed as a possibility for Member States only[i]. Considering that time is often of the essence in cases of fraud and financial crime, immediate rejection of an unsafe EDIW should also remain a possibility in high-risk use cases, such as exist in the financial sector.

2. The risk that the regulation focusses on a single technological solution

As stated above, the goal of the Commission is to create "*A technology where we can control ourselves what data is used and how*". The current proposal aims to implement this as EDIWs that will allow the user to store identity attributes only in the wallet. However, in some use cases it is necessary to let the verifier retrieve attributes directly from the issuer (originator/source) at the time they are needed[4]. It is therefore beneficial to make sure that methods used in these processes would also be subject to the regulation. This will prevent the use of current privacy-unfriendly systems in these situations, which would result in us having "*no idea what happens to our data*".

Processes that need to connect to the source come in different forms, but can usually be categorised as follows:

- Assuring greater up-to-datedness actuality or involving large datasets
- Processes in which user involvement is impossible
- Processes in which user involvement is impractical.

The proposal should leave open the option to pick between other types of implementations depending on the use case[ii].

If above use cases and appropriate methods are included in the regulation, this will mean they are required to follow the same or similar security and privacy enhancement, e.g., of the communication protocols used. To achieve the goals of the regulations, additional requirements are needed, such as:

- enforced consent before data can be shared
- guaranteed anonymity of verifier to issuer
- non-repudiation of interaction.

[3] For more details, please see In-depth Article - Loss of Control due to EDIW

[4] For more details, please see In-depth Article - More versatile EDIW

More information can be found on the website of the Partnership for Cyber Security Innovation (PCSI).

Call to action

To mitigate the concerns and keep digital interactions safe and current, two additions should be made to the eIDAS2 regulation:

1. Loss of control by forced acceptance of third-party identity wallets
    a. Add additional risk mitigation possibilities to alleviate the concerns raised regarding app certification.
    b. Expand the regulation to allow support for monitoring irregular behaviour and temporary rejection of EDIWs that are deemed unsafe.

2. A more versatile EDIW with a more diverse set of methods
    a. Add a provision to the EU reference architecture of EDIW for retrieving attributes at their source when an attestation is requested.

[i] Verkenning eWallets Speelveldanalyse, 11 January 2022 Innovalor, commissioned by the Dutch Ministry of the Interior and Kingdom Relations

[ii] SSI Speelveldanalyse, 1 October 2021, Innopay and TNO commissioned by the Dutch Ministry of the Interior and Kingdom Relations – Section 6.3

Partnership for Cyber Security Innovation is a collaboration of

ING ABN·AMRO
Belastingdienst achmea TNO
de volksbank ASML