EDPS

07 February 2023

EUROPEAN
DATA
PROTECTION
SUPERVISOR

The EU's independent data
protection authority

"Where are we heading with digital identities?"

Cybersecurity Standardisation Conference 2023

European Standardisation in support of the EU cybersecurity legislation

Wojciech Wiewiórowski
European Data protection Supervisor

Thank you for this invitation. Thank you for the opportunity to exchange views on **how standards and certification schemes can promote the trust and success of the European Digital Identity Wallet framework,** that is proposed by the revision of the eIDAS, or so called eIDAS 2 Proposal.

I would like to use this opportunity to make more general statements on 3 specific subjects which may bring some challenges, obstacles, or even mistrust, to our conversation between cybersecurity and privacy specialists, as well as in discussions between constitutional lawyers and protagonists of standard and formal specifications.

So, while the core of my presentation will contain the most important part of the EDPS' official position, it will not be surprising for most of the participants who followed the work done on digital wallets.

At the same time, three statements which I will make in the final part of this presentation may appear to be new and surprising for many of you. Despite the fact that at least two of them are pretty obvious and only the EDPS' negative approach towards them may surprise some of you, even though it is not the first time that I personally make all these three statements.

On the European Digital Identity Wallet framework

As our lives become more and more digital, **we need an efficient, secure and privacy friendly digital identity that will constitute the cornerstone of trust** between citizens, public administration, companies, public and private service providers.

In this context, I see a lot of opportunities for the **European Digital Identity Wallet framework to be a big success story**. This is why I have expressed at every opportunity **my full support for the objectives set out in the eIDAS 2.0 Proposal.** The relationship between the proposed framework and the GDPR can be examined under two different, yet complementary, aspects.

1) On the one hand, if implemented appropriately, it constitutes **a very effective safeguard for controllers to protect individuals and their data and comply with essential provisions of the GDPR**, such as data accuracy, exercise of data subject rights, and security of processing[1].

2) On the other hand, the **data processing activities related to the digital identity must fully comply with the GDPR**, in particular with the principles of data minimisation, and the requirement for data protection by design and by default.

From a data protection perspective, which I represent, it's, first of all, very important that this framework **enables citizens to have better and more transparent control** over their personal identities, with whom they share -their data, and for what purposes.

There is a reason why the digital identity must comply with data protection legislation, and that is to protect the rights and freedoms of individuals. We all know what the consequences

[1] *Identification and authentication of users in an IT system is one of the most important security controls. Thanks to secure access control, individuals are able to have access to their data with low risk of identity theft.*

are for citizens **if the digital identity is not implemented in the right way, with the appropriate safeguards**: identity theft and massive data breaches. But not only, a bad design can lead to excessive personal data processing and abuse of personal data that can have devastating financial, moral and physical harms for humans.

Data Protection principles embedded in the implementing standards

As I have already explained in my formal comments on the eIDAS Proposal, back in 2021, there are many challenges from a data protection perspective that must be faced, if we want this Proposal to achieve its full potential.

To be clear about my expectations: the **highest level of Security and Data Protection by Design and by Default** for the wallet framework is, for me, **the cornerstone of a Trusted Digital Identity**. I would however prefer a Proposal that had given **more insight into what to expect** from EU Member States' way of implementing eIDAS measures from **the common toolbox** that will be further developed.

In other words, I would prefer the data protection safeguards and **relevant data protection standards** to already be integrated in the eIDAS 2 Proposal, at least at a high level, as this would not only facilitate compliance with GDPR, but also increase the level of certainty and trust expected from the Regulation.

The Proposal provides for **28 Implementing Acts** (!!!), which will decide on the actual implementation aspects. What usually happens in practice when there are a lot of Implementing Acts, is that there is a lot of freedom on their implementation. The risk is having various committees and working groups to decide on important technical aspects and reference standard to implement.

On that basis, I have the following questions:

1) **Will these "various committees and working groups" work on the basis of universally-accepted standards, if any? Will "the design and default" be compliant with the GDPR**?

   and finally

2) **Are there any mandatory certification mechanisms** in place?

Apart from the 28 Implementing Acts, the proposed framework of the digital identity wallet is **decentralised and consists of four different categories of actors, for every EU Member State:**

- the European Digital Identity Wallet issuing authorities;
- the Trust Service Providers;
- the public or private digital service providers that rely on the European Digital Identity Wallet (=Relying Parties); and
- citizens who are the wallet holders.

I am aware that, together with the eIDAS 2.0 Proposal, the Commission planned to create a **toolbox** that would contain the technical architecture, the use cases and the reference standards to be used by the EU Member States in their efforts to comply with the new Regulation.

In my view, it is of utmost importance that this **Toolbox is compatible with the GDPR, and in particular to adhere to the principle of Data Protection by Design and by Default**. So, the real work for Data Protection Authorities starts now, and we should find all the European schemes that may help to harmonise this work amongst DPAs from all over Europe.

The Commission's Recommendation sets out a process, with **a very ambitious timeline,** to support a common approach for the eIDAS's implementation amongst the EU Member States, by involving relevant public and private stakeholders. In that ambitious timeline, I see immediately the **challenge of being able to stay on track, because of the following:**

- **universally accepted standards;**
- **certification schemes; and**
- **accredited certification entities that could certify the wallet issuing entities from both cybersecurity and GDPR perspectives.**

I can give you an example where a certification mechanism may not be compatible with the GDPR. There are many cases in which organisations have acquired an IT security certification, such as the ISO 27001, **they have the misconception that this automatically ensures compliance with Article 32 of the GDPR on the security of processing**. But this is not the case, and there must be **specific disclaimers for such certification schemes. In case the organisation process personal data, there are additional safeguards that may be required in order to ensure compliance**. For example, ENISA suggested in its EU Cloud Security scheme to have an 'extension profile', to also cover Article 32 of the GDPR, while collaborating with the EDPB CEH Subgroup.

Critical areas that need attention from the data protection perspective

Allow me now to address some important topics that are of vital importance to minimise data protection risks, when implementing the digital identity framework.

First, I have already expressed my serious concerns on the **data exchanges between wallet holders and digital service providers, the so-called Relying Parties.**

The only way we can protect personal identification data from excessive requests for data that is not necessary from the service providers is to define relevant reference standards, with precision, **which categories of data can be requested from the user of the Wallet, for specified use cases or purposes**. Some examples I can think of:

- If the purpose is **age verification**, the user could choose to submit their birth date but withhold the disclosing of other personal information that is not relevant to the purpose. Better, in most cases, the exact age might not be needed, if for example, the purpose is to identify an adult. An attribute stating that the individual is an adult, issued by a Trust Service Provider, would be enough.
- If the purpose is **legal identification**, for example in the banking or telecommunications sector, as required by law, the user could reveal only those pieces

of identity data mandated by law, without biometric identifiers, for example, if their processing is not explicitly required.

Another area that deserves careful thinking and exploring of possible alternatives is the technical and organisational design options for cross-domain and cross-border linking of identities, currently implemented though the so-called **unique and persistent identifier and the matching process**. This identifier inherently creates risks for individuals, such as full and possibly unnecessary ability to link personal data across sectors and actors (such as Relying Parties, Trust service providers), wide consequences in case of identity theft, surveillance, and of course abuse by marketing practices.

I am aware of privacy enhancing technical solutions that are based on cryptography, such as pseudonymous identifiers or pseudonymous electronic signatures. I do not have a particular preference for one of these techniques, but I think it is important that the standardising organisations address them carefully.

Conclusions

To sum up, the European Digital Identity Wallet is a project that is **not only** designed to make our digital lives easier, but that can also potentially create **additional benefits for our privacy and data protection**.

Whether this potential is achieved does not only depend on the Regulation, but also very much on the implementation and, in particular, on technical architecture, the reference standards and certification mechanisms that will be invoked. All these elements must be **compatible with the data protection legislation**, and in particular, with the principles of data protection by design and by default and the security of personal data.

I strongly believe that if citizens can make full use of both public and private online services seamlessly throughout the EU with the help of the ID Wallet, the use of platform based, often less data protection friendly identification solutions, could be rendered unnecessary, and this will be a big win for data protection.

Several minutes ago I said that however positive or at least neutral the attitude of EDPS can be towards the digital wallet itself and to the role of standardisation in this project, the more doubts remain, and they may have a negative impact on the cooperation with stakeholders. They may even create some mistrust on both sides.

First of all: the EDPS – like many other DPAs – often protested about the idea of general strong identification being the *conditio sine qua non* for the use of internet services. While identification might be necessary in some cases (financial services are the best example), it is absolutely not necessary for most of the Internet. There is however the tendency to push users towards identification - in theory to make services more secure, in practice to track users and to profile them.

If there was anything missing to make identification mandatory by some legal act, it was a universal ID tool which the digital wallet may provide the EU with. This is not what the digital wallet is for. If this is the piece of the puzzle which was missing for total surveillance online, then I will not support it.

Secondly, there is a gap between those who should represent society when the legislation balances our rights and obligations – namely legislators and parliamentarians as representatives of the citizens, and IT experts setting "standards *de facto*" – actually formal specification for the very product which – because of the scale of the project – become "standards *de facto*". Such disconnect is illustrated by the picture where the legislators delegate their powers in technical matters to the Commission that, in turn sub-delegates them to EU agencies, like EU LISA, or where the legislators state high level goals ("compliant with GDPR"), and experts should create the means.

The more I am afraid of such tendency, the more I see the bridge in standardisation, but keep my doubts on its preparedness as I said before. And the third threat to the nice picture we draw today. Before we make GDPR certification mandatory for wallet providers, let's check if the schemes exist.

And for this reason – good luck to the Luxemburgish Data Protection Authority and for certification bodies in the Grand Duchy, because they seem to be the only ones fully ready.

Thank you again for this great opportunity to discuss on such an important topic.