eIDAS 2.0: Comments before the start of Trialogue

13. March 2023

Non discrimination provision

The European Digital Identity (EUDI) Wallet can only be successful when it is the chosen tool that gains the trust of citizens to hold their most sensitive health, financial and identity information. Any obligation on people to use the system would undermine this trust and lead to a pushback that would in turn undermine trust. Additionally, many will simply be unable to use the EUDI Wallet because for example many senior citizens lack the technical skills to use it safely[1] and low-income households might lack the modern smartphone required to run the app.

Therefore, the non-discrimination provision in Article 6a(7a) is one of the corner stones of the Parliament's first reading position. A text like this was approved by all four committees in Parliament and enjoys extremely wide support across all political groups in the European Parliament. Of course, Member States would want the possibility to force users to use the Wallet in special cases, but it's up to the Parliament to protect the interests of citizens when it comes to the voluntary nature of the EUDI Wallet.

Regulation of use cases

Article 6b(1e) is vital for the prevention of fraud and identity theft. We can expect bad actors attempting to rely on the EUDI Wallet to establish themselves in countries most suitable for their criminal business model (forum shopping). If citizens complain about fraudulent transactions in the Wallet, their member state should have remedies at their disposal to stop such relying parties from participating with the EUDI Wallet and undermining the trust in the whole system. The proposed competency in Article 6b(1e) of the European Digital Identity Framework Board (EDIFB) to overrule the national eIDAS regulator helps rectify the long-standing problems of lack of enforcement in Ireland and other countries.

The handling of these cases by the eIDAS regulator is currently limited to the regulator in the country of establishment of the relying party, according to Article 6a(3)(ae)(iii) and Article 6a(7)(m). So far it's unclear in the text at which stage and in which cases the mandate of the EDIFB would begin and what procedural safeguards the user can rely upon to get access to justice and remedy cases of fraudulent transactions. In light of the important safeguard in Article 6b(1e) the complaint mechanisms in Article 6a(3)(ae)(iii) and Article 6a(7)(m) and the mandate and procedural rules on the EDIFB in Article 46c should be clarified in trialogue. The Parliament is absolutely right that an instrument like the EDIFB is needed to ensure harmonized implementation of the Regulation and establish a unified level of trust and functionality across the union.

The common interface requires in Article 6a(4)(a)(v) that the authentication and validation mechanism of the EUDI Wallet to be limited to "**approved** relying parties". Article 6a(4)(ca) talks about "embedded disclosure policies" for certain electronic attestations of attributes, but there is no definition of "disclosure policies" anywhere in the text. The problem this creates is that a relying party could go

1 Examples how Senior citizens could be left behind in digital transition in the Spanish banking sector: https://www.epe.es/es/activos/20230210/desaparicion-forzosa-cartillas-bancarias-acelera-82724455

beyond their registered use cases and ask the user for information that is improper, illegal or fraudulent. Such a scenario could only be detected if the user were to use the complaint mechanism in Article 6a(3)(ae)(iii) or Article 6a(7)(m), which might be only after the information was already obtained by the relying party and the damage is done. Importantly, the current text would allow the relying party to diverge from their registered use cases on a case-by-case basis and only in certain individual user interactions, so as to remain undetected by the public authorities (physical coercion, abuse of power, pay or consent, tying consent to the provision of a service, etc.).

Our suggestion would be to follow the intent of both Parliament and Council and re-introduce simple technical safeguards that limits the use of the EUDI Wallet according to the registration of the relying party in the country of establishment. The French Presidency proposed text to this affect in their proposal from 10 March 2022 for Article 6a(5)(e), which demands that: "[...] to ensure that the use of the European Digital Identity Wallet by relying parties is consistent with the intended use as registered in accordance with Article 6b(1)". Such language reduces the administrative burden for the national regulators and ensures predicability and trust for the whole EUDI Wallet ecosystem.

Unobservability of user behaviour

The EUDI Wallet is ubiquitous technology which can be applied to all areas of life by an unknown number of relying parties with an unknown set of attribute providers. The potential for tracking of user behaviour poses a severe threat to the privacy of EU citizens. A bird's eye view about all user transactions amounts to a panoptical situation in which health, financial, judicial sectors, as well as daily interactions in commerce and leisure activities could be observed from one central vantage point. This risk creates a severe hurdle in the uptake of the EUDI Wallet by privacy-sensitive citizens and it would undermine the expectations that a European system should adhere to privacy-by-design principles as established in the GDPR. Importantly, the European Parliament established strong unobservability in the 2021 EU Digital Covid-19 Certificate[2] and vaccination certificates are just one of many attributes foreseen in the EUDI Wallet.

The Parliament text is the only version of the bill that provides for the necessary safeguards to rectify this problem. This issue is central and cannot be left for delegated acts or technical implementations, which might change over time or for certain countries. Hence, safeguards in Article 6a(7)(f) about the architecture of the EUDI Wallet from the perspective of the issuer are vital, as well as provisions to protect against providers of attributes tracking the use of their attributes by the user in Article 6a(4)(b)[3] and about cloud storage of transactions in Article 6a(7)(c).

The architecture safeguard comes from the exclusive competency of LIBE and is currently worded very extensively:

> *"the technical architecture of the European Digital Identity Wallet shall prevent the issuer of European Digital Identity Wallets, Member State or any other parties from collecting or obtaining [...] information about the use of the European Digital Identity Wallet by the user [...] the European Digital Identity Wallet shall not allow providers of electronic attestations of attributes to track, link, correlate or otherwise obtain knowledge of transactions or user behaviour"*

2 Regulation (EU) 2021/953 Article 4(2)

3 A simple Example is universities tracking the use of diplomas issued to Alumni when they are shown to potential employers.

In the ITRE compromise negotiations Article 7a(7) achieves the same outcome, but was clearer and provides a more comprehensive text:

> *"(a) issuers and managers of the European Digital Identity Wallet shall not be technologically able to receive any information on the use of the European Digital Identity Wallet or its electronic attestation of attributes. For the purpose of protecting user data against loss or corruption, encrypted synchronization and encrypted backup functions shall be permitted, subject to the explicit consent of the user. The issuer or manager of the European Digital Identity Wallet shall not combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or manager or from third-party services which are not necessary for the provision of the Wallet services. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held. Where the European Digital Identity Wallet is issued by private parties, the provisions of Article 45f, paragraph 4, shall apply mutatis mutandis;*
>
> *(b) issuers of the electronic attestation of attributes shall not be technologically able to receive any information about the use of these attributes or about the use of the European Digital Identity Wallet;*
>
> *(c) relying parties shall not be technologically able to receive any information other than that which the user has explicitly consented to."*

Unique persistent identifier

The question of unique and persistent identifiers was discussed at length. Even the Council diverged from the Commission proposal because of the constitutional problems such a tracking identifier would create in countries like Germany and Portugal. France, the Netherlands and Austria have also raised concerns. The Parliament version of Article 11a and Article 6a(7)(g) provide for the necessary safeguards to limit the application of such identifiers to legal Know-your-Customer (KYC) requirements and cross-border scenarios of public institutions acting as relying parties. The Parliament version would still achieve the required unique identification in those cases, but prevents this identifier being abused for tracking purposes. Importantly, this issue was also dealt with by the Parliament in the minimum personal data set in Article 12(4)(d).

The Commission has provided a text suggestion to Council and Parliament that only appears to tackle the problem: "Member States shall provide for technical and organisational measures to ensure the protection of personal data and prevent profiling of users". The technical reality is that as long as such a unique and persistent identifier exists and is exchanged, that relying party will be able to use it to track that user across interactions and sectors. There are no technical or organisationsal measures that could prevent this identifier from being abused for tracking. Sector specific identifiers are similarly not a solution because social media sector identifiers would make it even easier than it is now to correlate user behaviour and preferences across services.

Open source provision of the Wallet

Article 6a(2a) is an important provision that enables trust in the EUDI Wallet by making the source code available for independent review.

Privacy by design functions

The Parliament version of the bill enshrines that privacy-friendly functions of the EUDI Wallet like zero-knowledge proofs are clearly rooted in the text and are also given preference over more privacy intrusive functions of the EUDI Wallet. If we aim for user trust, it is vital we promote modern functionalities that enable requirements like age verification without any negative consequence for the privacy of citizens. In this regard the provision in Article6a(4)(a)(vi), 6a(7)(k), Recital (6b) and Article 3(5c) are vital.

Right to pseudonymity and relationship to the GDPR

Article 5(1) establishes important clarity about the relationship of the eIDAS regulation to the GDPR. It is vital that the high EU data protection standards are adhered to by this critical system.

The success of the EUDI Wallet shouldn't lead to a higher risk of over-identification. With the proliferation of easily accessible and cheap identification technologies in all sectors of society the Parliament has to ensure that everyday interactions of citizens, which currently can be done anonymously or pseudonomously, will not be undermined by this legislation. Therefore, the safeguards in Article 5(2) that **freely chosen pseudonyms** must be available to users whenever there is no legal requirement to provide their identification are vital for the impact this Regulation will have on millions of citizens.

Blind proxies

Article 6b(3a) is an important safeguard that prevents the centralisation of user interaction via companies that offer point of sales terminals or online libraries for integrating the EUDI Wallet in existing eCommerce systems. This legal safeguard ensures that a technology is chosen that prevents this problem from even emerging.

Obligations for certain relying parties to support the EUDI Wallet

We are strongly in favour of limiting the obligation for relying parties to offer the EUDI Wallet to their users or visitors to those relying parties under a legal KYC requirement, according to Article 12b(2). The terms of service should not be sufficient grounds to offer the EUDI Wallet in order to identify the user. Relying parties will still be free to offer the EUDI Wallet, but at their own discretion. From a data protection perspective any identification via the EUDI Wallet should at best be limited to cases of legal KYC requirements and not be based on terms of services.

Very large online platforms (VLOPs) according to the Digital Services Act have a special obligation to support the Wallet for logging into their service. The toxic surveillance-driven business models of these Big Tech companies require special safeguards to prevent the EUDI Wallet to contribute to privacy infringements common with these services. Article 12b(3) makes attempts in doing so with a particular right to pseudonymity and an obligation to separate EUDI Wallet data from all other data, except if specifically requested by the user.

We are in favour of the inclusion of civil society in the creation of self-regulatory codes of conduct in Article 12b(4).

Further reading

We already provided analyses of the Council General Approach[4], the ITRE compromise amendments[5], the Architecture Reference Framework[6] and the original Commission proposal[7]. In an open letter 39 civil society organisations, academics and independent experts from all around the world have called on the European Parliament to ensure the eIDAS reform respects fundamental rights and creates a trusted environment for user data[8].

We remain available to all interested parties in this reform for further conversations and public scrutiny.[9]

4 https://en.epicenter.works/document/4384
5 https://en.epicenter.works/content/european-digital-identity-a-potential-game-changer
6 https://en.epicenter.works/document/4566
7 https://en.epicenter.works/document/3865
8 https://en.epicenter.works/document/4536
9 https://en.epicenter.works/contact