Dear Members of the European Parliament,
Dear Permanent Representatives to the European Union,
Dear European Commission,

4. September 2023

The current trilogue negotiations on the eIDAS Regulation[1] are at a critical stage. Recent proposals by the European Commission to remove essential safeguards are alarming. In the current trajectory the European Digital Identity (EUID) Wallet is **not safe to use** and as members of civil society and Europeans that care about privacy we would have to warn citizens against using it.

The proposed removal of the right to pseudonymity in Article 5 starting at row 104 is a gift to Google, and Facebook. Without a strong right to freely choosen usernames the surveillance business model of Big Tech will soon have the legal names of all EU citizens that use the EUID Wallet. Facebook's long standing goal to have everyones real legal name would be compulsory when row 104 and 104a aren't adopted in line with Parliaments mandate. As highlighted by the EDPS in February[2], protecting against the risk of over-identification can only be achieved by strong regulation of use-cases that doesn't leave it up to the ToS which data users have to hand over when they want to use a service.

The Commission also proposes to delete the non-discrimination provision in Article 6a (7) (7a) in row 135m, which would open the door to compulsory use of the EUID Wallet in many sectors. This vital safeguard currently prevents the elderly, young people without smartphone or less digitally savvy parts of the population from being excluded or hindered for not using the new EU system. Without it, users would no longer be free to choose between the Wallet and other means. We already observe such discrimination in the form of higher prices for eGovernment services[3], if people rely on analog means to obtain services. This **non-discrimination protection needs to be upheld** for an inclusive digital public infrastructure in order to allow real user-choice, which was the promise of Commissioners Vestager and Breton when announcing this proposal[4].

It is alarming that the Commission proposes to remove core privacy protections from the EUID Wallet. The Parliament has adopted a safeguard in row 135e to protect concrete user behavior on the Wallet from being observed by the Member State who issues the Wallet. As the Wallet will span across all areas of life such **unobservability** is a vital architectural safeguard. Without this safeguard, everything that happens on the Wallet – like public transport movements, social media logins, doctor visits and financial behavior – can be observed. The COVID-19 digital certificate contained exactly this safeguard and as the Wallet will supersede such health certificates, the Commission is actively removing safeguards upon which the user could previously rely[5].

The council proposal for an Article 32a starting in row 317a in conjunction with Article 6a (4) (b) in row 126 would allow Trust Service Providers (TSP) to observe every user interaction with the EUID Wallet. While the user only wants to share information about themselves with a particular relying party, the TSP would know about everything a user does with the Wallet. Validation can happen in many other ways without forcing the relying party to contact the TSP with the concrete data and user information. This architecture would be the **opposite of privacy-by-design**. We support the Parliament's position in row 126 and oppose the Council's wide-ranging extension of the roles and business models of TSPs. The Commission's proposal on row 126 was much closer to the Parliament, yet they abandoned it in favour of the Council text. This is not a balanced solution in service of the people.

[1] 2021/0136 (COD)

[2] https://edps.europa.eu/system/files/2023-02/23-02-07_ww-enisa_en_2.pdf

[3] https://www.wien.gv.at/english/e-government/transportation/parking/residents/parking-permit.html

[4] See "who wants to use it" https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

[5] https://en.epicenter.works/document/3865 (page 3)

Europe has a central role to play in demonstrating how a digital identity system can incorporate privacy-by-design and be widely trusted. While the Commission's proposal only included the concept of selective disclosure, the Parliament has actually reflected the current discussion in academia and global standardization bodies by introducing the concept of **Zero-Knowledge-Proofs**. Such an approach is a win for citizens, as it allows confirming facts about them without revealing the underlying information[6]. These are the types of functions that will decide if the Wallet is a privacy-friendly technology or not. The Commission is proposing to delete Zero-Knowledge-Proofs in row 125f and 135j. Their justifications that Zero-Knowledge-Proofs are not technology neutral and not safe against quantum cryptography attacks are wrong, as for several years this has been the main focus of academic research for any privacy-friendly digital identity solution[7].

We also see the Commission aligning itself with the business interests of vendors of digital identity software to the detriment of transparency. While the Parliament proposed the Wallet to be **open source** so as to allow public scrutiny and earned trust based on the actual functionality of the software, the Commission acknowledges how useful this could be, but aligns itself with the Council by moving open source from row 116a in Article 6a (2) to a non-binding Recital 11aa.

Lastly, the Commission also wants to delete row 135k which clarifies that the issuer of the EUID Wallet is also the controller of the processing of personal information. Simply put, they justify this by "GDPR applies anyway". First and foremost, this wasn't clear to the co-legislator as references to the GDPR were actually removed by the Commission and thankfully later re-introduced. Secondly, the GDPR obliges lawmakers to name the controller or set forward guidelines how to determine the controller, whenever legally mandated processing of personal data is carried out. It's exactly because the GDPR applies that row 138k is necessary for eIDAS to fulfill requirements of the GDPR.

These are just a few of the many red flags we want to point your attention to. We remain at your disposal and look forward to future exchanges on this file.

Sincerely,
Epicenter.works – for digital rights

[6] e.g. proof a person is above 18 without revealing their birthdate.

[7] Together with the possibility of binary encoding of properties of certain attributes, such as the over_18 etc. derivations of date of birth attributes, mDL authentication key rotation provides properties of zero knowledge proof of attribute properties. See Annex E.8.4 of the ISO-mobile driving lisence standard.