Dear Swedish Presidency and Permanent Representations of EU Member States,
Dear Rapporteur Romana Jerković and Members of the European Parliament,
Dear Executive Vice-President Commissioner Vestager and Commissioner Breton,

20. June 2023

The 24 undersigned civil society organisations, academics and research institutions urge you to reconsider the current trajectory of the reform of the eIDAS regulation[1]. Without essential privacy and non-discrimination safeguards, the European Digital Identity Wallet will create an unprecedented risk for every European in their online and offline life.

The current trilogue negotiations have distinguished poorly between legitimate use cases and fraudulent or abusive scenarios. The regulation lacks redress for national eIDAS authorities to act against bad actors and expel them from the eIDAS ecosystem.[2] Privacy-respecting functions are not given preference over intrusive functions of the Wallet. Legal Know-Your-Customer requirements of banks and insurances are put on an equal level as the surveillance driven business models of Big Tech.

In its current form, the European Digital Identity System would be a gift for Google and Facebook to undermine the privacy of EU citizens. This will impact everyone in the EU and put them at a lower privacy level than people in other world regions.

Today, we are surveilled based on illegal device fingerprinting. All our clicks and touches are fed into behavioral profiles about us. Soon the eIDAS regulation might introduce a unique and persistent identifier for every citizen that allows the same Big Tech actors to correlate our behavior across the public and private sector with unprecedented accuracy. No technical or organizational measure can prevent the large-scale abuse of such a serial number for humans.[3]

Today, in many everyday situations citizens can make use of their right to freedom of expression and freedom to conduct business in anonymity or pseudonymity. The European Digital Identity Wallet has the potential to eradicate these opportunities to withhold legal identification and lead to a constant threat of over-identification in everyday interactions and a real name internet.

Whenever no legal basis obliges the identification of a person, the right to pseudonymity should be upheld when using the Wallet.[4] It would not be acceptable to make the use of pseudonyms the exception and the identification of users the norm. Similarly, when identification is not legally mandated, attestation of attributes should be done with Zero Knowledge proofs.[5] If the EU wants to

1 2021/0136(COD)
2 Effective Redress should empower national eIDAs authorities to act on consumer complaints and expel relying parties irrespective from their country of establishment. If not, the GDPR enforcement nightmare repeats.
3 This problem is not limited to Article 11a, but extends to the minimum PID in Article 12(4)(d) and was also a massive flaw in the first version of the toolbox from the eIDAS expert working group https://en.epicenter.works/document/4566
4 See Article 6b(3) in the European Parliament Mandate
5 See Article 6a(7)(j) in the European Parliament Mandate

set a positive world-wide standard with the Wallet, it needs to uphold its own GDPR principles of privacy-by-design and privacy-by-default.[6]

To ensure the political promise that the Wallet will remain a voluntary system for natural persons, a non-discrimination provision should ensure that nobody be excluded or hindered for not using the Wallet. Such a provision was adopted in all four committees in the European Parliament with a huge majority across the aisle.[7] We urge Council to support such a right of equal participation in society across the digital divide, in particular for the benefit for senior citizens and low-income households.

The trust users will place in the Wallet heavily depends on effective enforcement of rules governing what relying parties are allowed to ask from users. Putting all the burden on the shoulders of citizens by solely relying on informed consent would be impractical given known GDPR shortcomings[8] and the sensitive nature of information stored in the Wallet[9]. A solution put forward under the French presidency[10] is to require relying parties to register the information they intend to inquire from users for any particular use case. Together with a technical limitation of the Wallet according to this registration, a balanced, cost-efficient and low-bureaucracy system emerges. The EDPS outlined such a system and called it: “The only way we can protect personal identification data from excessive requests“[11].

Lastly, we want to highlight the potential that the European Digital Identity Wallet could become a single point of failure to critical infrastructures. By tying all eGovernment interactions, visits to the doctor, banking, social media logins, public transportation and many other sectors to the Wallet as the sole key, even a minor downtime of this system could have serious consequences. Sensitive identity, financial and health information of millions of Europeans offers a lucrative attack surface that makes cybersecurity attacks very likely. This strong centralization could prove a fatal mistake.[12]

With proper safeguards the European Digital Identity Wallet has still the potential to become a very powerful, fundamental rights respecting and privacy-preserving ubiquitous platform for digital interactions. The success of this system will ultimately depend on the level of trust citizens put in it. Therefore, we believe it is in the interest of all negotiating parties to consider safeguards outlined in this document.

Sincerely,

epicenter.works – for digital rights (Austria)
European Digital Rights (Europe)
Privacy International (Global)

6 See Article 5(2) & (3) in the European Parliament Mandate to guide implementing acts and national technical specifications, while these principles are also enshrined in the two aforementioned provisions.

7 See Article 6a(7a) in the ITRE report, Article 6a(10a) in IMCO, Article 6a(6a) in JURI and Article 6a(7a) in LIBE

8 Prohibition of tying is broken on a massive scale, pay-or-consent schemes pervert informed consent and in many offline situation power dynamics will undermine the free choice of users.

9 European Health Data Space 2022/0140(COD)

10 See Articles 6a(5)(e) and 6b(1) of the Council Compromise from 6th June 2022.

11 See EDPS speech from 7. February 2023, page 4

12 This problem would be exacerbated if the Wallet shall also be used for the Digital Euro https://www.euractiv.com/section/economy-jobs/news/leak-eu-commission-wants-digital-euro-accessible-to-everyone/

Electronic Frontier Foundation (Global)
SSI Korea (South Korea)
Homo Digitalis (Greece and EU)
IT-Pol (Denmark)
Državljan D / Citizen D (Europe)
TEDIC (Paraguay)
ApTI - Asociatia pentru Tehnologie si Internet (Romania)
Metamorphosis, Foundation for Internet and Society (Europe)
Digital Society, Switzerland (Switzerland)
Big Brother Watch (UK)
Montesquieu HOUNHOUI (Benin)
Elektronisk Forpost Norge (Norway)
Charlie Martial Ngounou (Africa)
Digital Access (Central Africa)
Asociación TEDIC (Paraguay)
Fundación Karisma (Colombia, Global)
SlashRoots Foundation (Caribbean)
Temple University Institute for Law, Innovation & Technology (Global)
Jaap van der Straaten (Global)
Jose Maria Arraiza (Global)
Verónica Arroyo (Global)