

Dear Executive Vice-President Henna Virkkunen,
Director-General Roberto Viola,
Director Christiane Kirketerp de Viron,

Brussels, 10th of March 2026

Open letter concerning the fourth batch of eIDAS Implementing Acts

The undersigned digital rights and consumer protection organisations would like to thank the Commission for its continued work on implementing Regulation (EU) 2024/1183 (the eIDAS Regulation). However, we underline that the European Digital Identity Wallet (EUDI Wallet) can only succeed if it guarantees strong privacy protections, legal certainty and harmonised trust across the Union.

With this letter, we wish to raise serious concerns regarding the fourth batch of Implementing Acts. Our detailed legal and technical analysis is available [here](#).¹ We are concerned that, in several respects, the latest draft Implementing Acts being consulted upon not only fail to resolve previously-identified shortcomings, but also risk weakening some of the core protections enshrined in the eIDAS Regulation itself. This is rendered all the more urgent by the multiplication of proposed use cases for the EUDI Wallet (such as age-gating online services).

1. Registration certificates must be mandatory

The co-legislators designed the EUDI Wallet such that, if a request for information-provision exceeds the scope needed for the service provided (“over-asking”), it triggers an automated warning on the person’s Wallet. This automated trigger relies on a system of registration certificates – whereby services (relying parties) state in advance what their intended use of the EUDI Wallet will be, and which data points they will need to request from users for this; this statement is then then examined and recorded by the Member State in which the relying party is established. However, under the current version of the Implementing Acts, this safeguard is cancelled-out because registration certificates are made optional. Each Member State must thus decide whether they implement the certificate system or not, a decision which may render them more attractive as country of establishment for relying parties. And if even only *one* Member State decides not to require registration certificates, the benefits of registration certificates would then be voided for all users in the EU.

For instance, a relying party could offer age verification services, for which no other data than the person’s age would be needed; if established in a Member State which doesn’t issue registration certificates, the relying party would be able to discreetly request additional data, such as the person’s legal identity, from all or just selected users. Users would either blindly trust the request because they expect to be automatically warned of over-requests, or – if they know of the loophole – they would have the burden of scrutinising each and every request going through their Wallet, in fear it comes from one of those weaker Member States. This therefore undermines user trust in the entire

¹ <https://epicenter.works/content/eidas-amendments-to-the-implementing-acts-batch-4-rev8> and https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16113-European-Digital-Identity-Wallet-registration-of-wallet-relying-parties-update/F33378018_en

ecosystem and puts some relying parties at an unfair advantage, both of which contradicts the goal of eIDAS.

The prohibition of “**over-asking**” by relying parties can only be enforced effectively if wallet-relying party registration certificates are mandatory in all Member States. This issue has been separately raised in an open letter signed by 15 consumer protection and digital rights NGOs². While the Commission did address it after the consultation, the adopted drafts reintroduced it³.

2. The right to use pseudonyms must be fully safeguarded

The eIDAS Regulation clearly protects the right of users to rely on pseudonyms where identification is not required by law⁴. However, the current draft Implementing Acts narrow the scope of this safeguard, and enable “**over-identification**”, particularly in remote online contexts. Concretely, with the current wording, it is possible for relying parties not to offer a pseudonym-based interaction to users, and instead to systematically request the legal identity of the user despite it not being needed, without having to justify themselves.

To address this, relying parties must therefore clearly declare whether a specific use case is subject to a legal identification obligation, and specify where that obligation comes from.

3. Mandatory biometric data would be disproportionate

The draft Implementing Acts now propose to include a mandatory facial image in the Wallet’s minimum person identification data set. This would mean that all use cases in which a user uses the Wallet to identify themselves to a service would necessarily entail the transfer of this sensitive personal data. This represents a fundamental and disproportionate expansion of sensitive data processing. Such a change significantly alters the privacy implications of the Wallet, goes against the intentions of the co-legislator (who removed language on biometrics from the Regulation) and should therefore be removed.

4. Do not dilute obligations of very large online platforms

The eIDAS Regulation obliges Very Large Online Platforms to accept and facilitate the use of the EUDI Wallet, including the use of pseudonyms⁵. However, the technical specifications (WebAuthN and PassKeys) of the proposed Implementing Acts would enable these companies to limit themselves to fulfilling a restrictive interpretation of this obligation and allow existing (proprietary) passkey implementations to substitute for genuine EUDI Wallet integration.

If these loopholes are not closed, the user’s right to pseudonyms could consequently be made void, and the management of sensitive credentials could be completely outsourced to non-EUDI Wallets, rendering the eID technical safeguards mostly useless for this specific use case.

2 <https://epicenter.works/en/content/open-letter-eidas-implementing-acts>

3 <https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-2-rev6> and Implementing Regulation (EU) 2025/848

4 Article 5 and 5b(9)<https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-2-rev6> and Implementing Regulation (EU) 2025/848

5 Article 5f(3)



European Digital Rights



5. Preserve strong unlinkability standards

The eIDAS Regulation sets high standards for ensuring that a person's use of the EUDI Wallet cannot be tracked and linked to their identity ("**unlinkability**")⁶. If, through the EUDI Wallet, a person uses their government-provided identity credentials on a porn website – to prove their age, for instance – this specific 'transaction' should not be traceable, neither by the government nor by the porn website.

However, the proposed Implementing Acts weakens this crucial obligation. The eIDAS Regulations' "shall not allow" tracking/linking/correlating becomes mere safeguards "hindering" linkability and traceability, in the Implementing Act. This weakening of security obligations will translate into a legitimate weakening of trust into the Wallet. We call for stronger language to be used.

The European Digital Identity Wallet will only gain public trust if privacy and user control are embedded in its technical and legal architecture from the outset. We therefore respectfully ask the Commission and Member States to address these concerns in the upcoming comitology discussions and to ensure full alignment with the eIDAS Regulation.

We remain at your disposal for further exchange.

Sincerely,

epicenter.works – for digital rights

European Digital Rights (EDRi)

AK EUROPA

Homo Digitalis

Initiative für Netzfreiheit

IT-Pol Denmark

ApTI Romania

Vrijdschrift.org Netherlands

Chaos Computer Club e.V.

Digitale Gesellschaft e.V. Germany

6 Article 5a(16)