EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Digital Society, Trust and Cybersecurity
The Director

Luxembourg
CNECT.H.4.002/VAN

Mr. Hannes Stummer
Email: [redacted]@epicenter.works

Dear Mr Stummer,

Thank you for transmitting the open letter from a number of civil society organisations and individual experts of 7 August 2024, which conveys concerns regarding appropriate safeguards for user privacy and security in relation to the Architecture and Reference Framework for the European Digital Identity Wallet.

I would like to start by reassuring you that the Commission takes the issue of privacy and cybersecurity very seriously.

The European Digital Identity Framework will offer citizens a secure and trustworthy framework to identify and to share digital data online. Protecting the privacy of users and safeguarding their rights to their personal data is the fundamental principle driving the work of the European Commission when designing the implementation framework, in accordance with the legal act establishing the European Digital Identity Wallets.

The European Digital Identity Wallet provides the user full transparency and control over personal data shared through the wallet. The user will be able to use selective disclosure in order to determine exactly which data should be used and with whom. In addition, the user will be able to see all transactions recorded in an electronic dashboard and may ask for the deletion of data with service providers at any time. Complaints to data protection authorities in case of a suspicion of data misuse will equally be possible by means of the wallet. These possibilities fully implement the rights of users under the GDPR and are complemented by a number of legal safeguards included in the European Digital Identity Regulation that require service providers to strictly separate identity data and wallet issuers not to combine data unless the user explicitly requests this.

The privacy of users will be guaranteed fully protected by the European Digital Identity Wallet. For this purpose, pseudonyms generated and stored safely by the wallet can be used and the Regulation requires relying parties to accept them. The only possible exception for this, as established by the regulation, is when identification is required.

Regarding your statements linked to the proposed cryptographic mechanisms and the key privacy requirements for unlinkability, unobservability or zero knowledge proofs, we would like to emphasise that the technical specifications proposed for the wallet include the latest technical standards and solutions available today. These specifications foresee that the wallet

uses privacy preserving techniques, which ensure unobservability where the identification of the user is not required. For example, the technical protocols used by the wallet will prevent that the issuers of certain data can trace how this data is used later on. In addition, the technical infrastructure of the wallet will be designed to ensure that only the minimal necessary amount of data is transferred and that links between the different transactions cannot be established.

In addition, the European Commission is working closely with a team of leading cryptographers in order to integrate into the wallet advanced privacy-enhancing technologies including zero-knowledge proofs. In this context, zero-knowledge-proof verification mechanism which can be implemented in secure hardware using secure cryptographic algorithms will be specifically developed for the wallet. These verification mechanisms would become a default standard in the future, and this will further improve privacy safeguards for the user. The implementing rules include a specific reference to their update in line with technological development.

Furthermore, to protect the user against illegal information requests, the technical framework for the wallet establishes very clear rules on which information can be requested from wallet users. For instance, any data request must be linked to a specific purpose and comply with the registration of service providers at national level. This obligation reflects the "purpose limitation" of the GDPR. Any request from relying parties on data other than data registered in the relying party registers would be clear breach of the Regulation which is directly applicable in Member States.

Additionally, as already mentioned above, redress in case of misuse is available directly through the wallet, full transparency is provided by means of a transaction log detailing which data have been shared, with whom, and for what purpose.

Regarding the identification of users by the law enforcements agencies, I would like to be very clear that the wallet does not contain specific features for this purpose. The ability of law enforcement authorities to identify users depends on national law. These laws provide for the conditions and processes under which such access is permitted, ensuring that it aligns with national legal frameworks and respects individual privacy rights. Processing of personal data for national security activities or law enforcement is out of the scope of the General Data Protection Regulation (GDPR) that guides the design of the wallet.

I would also like to reassure you that the wallet will be issued based on the same highest standards of security and trustworthiness in all Member States. As foreseen in the regulation, all wallets will be independently certified to a common methodology to ensure this. The Commission has requested that the EU cybersecurity agency, ENISA, develops a common certification scheme based on the Cybersecurity Act. In this respect I would also like to underline clearly that there cannot be backdoors in the wallet to allow for the re-identification of users by third parties. This would simply run counter to the fundamental principles of cybersecurity certification.
Finally, let me stress that the implementation timeline for the European Digital Identity Wallet is established in Regulation (EU) No 910/2014 and cannot be changed. As you mention, commitment to respect deadlines is an important part of building public trust.

The Commission is fully committed to establish a highly secure ecosystem for the European Digital Identity Wallet which fully enforces the rights of user to data and privacy and inspires the trust of citizens. The Commission will not hesitate to address swiftly and forcefully any infringement of the regulation, which would undermine the privacy and protection of fundamental rights.

Finally, we are committed to ensuring an open and transparent dialogue with civil society about the wallet implementation. I would therefore be happy to organise a meeting to discuss further your concerns and inform you about the ongoing work on the implementation of the wallet.

Yours sincerely,

Christiane Kirketerp de Viron
acting Director