eIDAS Quick Analysis: Implementation Acts

19. November 2024

The following are the relevant changes in the latest draft of the implementing acts for Article 5a of eIDAS. The basis of this analysis is the text that was sent out by the European Commission on 15. November 2024 and will be voted on 21. November[1]. The text has since been leaked by the Austrian parliament[2]. For ease of understanding, this document should be read in conjunction with previous submissions[3] on this dossier.

1. Unobservability

By withdrawing an addition in the definition of 'wallet instance', it is now once again ensured that the transaction logs only remain on the end user's device. Previously, information about the concrete usage behaviour of all users of the Wallet would have been visible to the wallet operator via the storage of all transaction logs on the server. This contradicts the principle of unobservability as laid down in Article 5a(14) and Recital 32 of the Regulation. This amendment reflects our recommendation and is deeply appreciated.

2. Use Case Regulation

The registration of relying parties that includes the attributes they intend to request is now is reflected in the introduction of 'wallet-relying party registration certificates'. Thanks to amendments in Articles 2 and 3 in the implementing act on protocols and interfaces, the user is now at least warned if the relying party goes beyond their registration. According to Article 5b(3) of eIDAS such requests for information going beyond the registration are illegal. Individual member states can now go further and completely prevent such illegal queries from being presented to the user at all. This is not the optimal solution, but at least an architecture that allows to protect users and that can prevent the repeat of a cookie-banner disaster.

3. Selective Disclosure

If consumers are confronted with requests for information, they have the right under eIDAS to answer them completely, not at all or partially/selectively. This principle of selective disclosure was not previously included in the implementing acts and has now been adopted with the wording from our proposed amendments in Article 3 of the implementing act on protocols and interfaces.

One fly in the ointment is that in Article 14 of the implementing act on integrity and core functionalities, the use of a pseudonym still goes hand in hand with the transfer of personal data requested without the need for separate consent.

1 https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD%282024%292116/consult?lang=en
2 https://www.parlament.gv.at/dokument/XXVII/EU/199076/imfname_11416115.pdf
3 https://epicenter.works/content/eidas-implementing-acts-european-digital-identity-wallets and https://epicenter.works/en/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19

4 Right to Pseudonymity

Article 14 of the implementing act on integrity and core functionalities has unfortunately not adopted our recommendations. Instead, recital 14 simply reiterated the wording of the Regulation. The technical standard in Annex V has also changed here from WebAuthn to Verifiable Credentials. Even after consulting with several negotiators, there is confusion as to how exactly this is meant to work for authentication and attribute attestation.

What really worries us is that there is still no technical way for the wallet to find out whether a specific use case is subject to a legal obligation to identify the user (KYC). However, such a distinction is necessary in order to ensure the right to pseudonymity in all non KYC cases.

5. Expansion of Databases

The Annex to the PID contains two new optional data fields: e-mail and telephone number. These two unique identifiers cause us great concern and were only added in the very last version of the text. It is questionable how these two data fields are to be collected by public authorities with a high level of assurance and what use cases we will see for them.