Analysis of the eIDAS Trilogue From 5. & 6. September

Based on the 4C document after the technical meeting on 5. & 6. September

Overview

We outline the most important changes from a citizen and data protection perspective. Other crucial issues remain open in trilogue and can be found in our open letter to the negotiators from 4. September[1].

We can expect major decisions in the next negotiation session on 15 September 2023.

Evaluation

🟡 **Pseudonymity** in Article 5 is improved by adding "freely chosen". There is still no right to pseudonimity, but it can't be prohibited without a legal KYC obligation. (row 104) Row 144 phrases the pseudonymity more strongly as a right but fails to include "freely chosen" pseudonyms. If users can't "freely choose" pseudonyms, they would be created by the Wallet and allow the governments to re-identify users online to their legal identity. Council raised objections while EP wants to keep as is, both rows could still change.

🟡 The obligation for Member States to offer an EUDI Wallet to their citizens & residents has been **postponed** to only kick in **24 months** after the delegated act which outlines the functioning of the Wallet has been adopted. Realistically, that means 2027! (row 112)

🟡 Parliament demands the EUDI Wallet to be **open source**. This is still not decided. The current proposal is a tiny step forward as it states "the source code of the application software components" of the EUDI Wallet shall be open. Council has reservations around IP rights and "incentives for private sector" and will get back with a proposal that excludes external service providers. (row 116a)

🟢 Slight positive improvement in the general description of the EUDI Wallet that combines all good proposals from EP and Council. "**User-friendly**", "**transparent**", "**traceable by the user**", "**under the sole control of the user**", "**while ensuring that selective disclosure is possible**". (row 118)

🟢 The **local generation and storage of pseudonyms** was adopted. EC still has reservations. (row 118c)

🟡 **Peer-to-peer functionality** of the Wallet has been approved. Unclear if such uses would be a way to undermine the requirements in Article 6b. EC still has reservations. (row 118d)

🟢 **Privacy dashboard** in the EUDI Wallet with full history log about all information sharing (requests). This includes complaint to the national DPA where the relying party is established. The establishment of a complaint mechanism is good, but complaint to the eIDAS regulator or remedies like the exclusion of a relying party of the eIDAS ecosystem would be more effective. Question: What about non-EU relying parties? (rows 118e to 118h, as well as row 125h and 125i)

🟢 **Download of user data and data portability** are agreed upon. The former is limited "to the extent technically feasible".

1 https://en.epicenter.works/document/4850

🟢 EUDI Wallet can **authenticate relying parties** and check their registration according to Article 6b. (row 125d)

🔴 **Zero-knowledge** as a function of the Wallet has not been agreed on yet. The EC is heavily opposed and only wants this as a recital. Thus, the Wallet would not be private-by-design and could be outdated already on the day of release. We touched in our previous open letter why many of the arguments from EC are not supported by academic literature. (row 125f)

🔴 The **registration of the relying party** is **no longer technically binding** what can be asked from a user via the Wallet. If a relying party goes beyond their registration and asks for more information, the user is simply "informed" but the request is not prevented. This paragraph is inconsistent with the text in Article 6b, but since both are not finally agreed on there remains hope. (row 127a)

🟢 The reference to the **unique persistent identifier (UPI)** was not just removed in Article 11a, but also in the reference to Article 12(4)(d). This is not new, but still good and we feared they might overlook that. (row 129)

🟢 **Issuers** of the EUDI Wallet are obliged to offer **easily accessible support to users**. (row 133g)

🟡 There is an **obligation for relying parties to register** their use case, including the data they want to request from users. EP is pushing for this, but Council so far objects. Commission seems constructive and wants to propose text on this point. We still have huge loopholes in the user case regulation as it's also unclear what happens if a relying party breaches their registration by requesting additional information (like health data) or acts in bad faith. There seems to be agreement on the obligation of relying parties to be identifiable before the user before requesting information from them. Exceptions from the obligation to register could come in the form of national legislation. (row 142 to 143a)