Some observations and questions on the European Digital Identity Architecture and Reference Framework

Eric Verheul (www.linkedin.com/in/eric-verheul)

28 February 2022

On 3 June 2021 the European Commission published an update of the eIDAS regulation in which a wallet (eIDAS wallet) plays a prominent role. On 22 February 2022 the European Commission published an European Digital Identity Architecture and Reference Framework (ARF). The ARF outlines a summary description of the eIDAS expert group's understanding of the eIDAS wallet concept.

I think the eIDAS Wallet ARF is a nice document shedding light on some (but not all!) unclear issues in the eIDAS update proposal itself I identified here. It might be interesting to a make a full comparison. As a first start let met state some observations and pose some questions on the ARF:

1. In meeting the eIDAS High authentication mechanism requirements, the ARF also refers to the use of Trusted Execution Environments (TEEs). This seemingly hints that the use of the Apple Secure Enclave and Android hardware backed keystore is acceptable. As this would open the wallet for >90% of the European citizens that would be good news. However, no further light is shed on eIDAS High authentication mechanism requirements. For this the ARF simply refers to the eIDAS implementation regulation CIR 2015/1502. This is meaningless as CIR 2015/1502 does not define the fundamental notion 'resistance to attack (High) potential' apparently due to the differences among the member states. But as this needs to be resolved for the eIDAS wallet public certification scheme (Article 6c of the update), I would suggest you start the discussion here and now. It is long overdue anyway.
2. What is the difference between "PROVIDERS OF PERSON IDENTIFICATION DATA (PID)" (Section 3.3) and the (qualified) "ELECTRONIC ATTESTATION OF ATTRIBUTES PROVIDERS" (Sections 3.5, 3.6)? It seems logical to me that a PID only provides "signed" personal data without the user being able to show he/she is the owner of it, at least in a online fashion. A digital driving license would be an example of this; it is signed by a government organization (RDW in the Netherlands) including the facial image of the holder. 'Authentication' then is based on a relying party comparing the image with the person showing it. However, the text on p. 19 "Online sharing shall require the user to prove ownership of the used (Q)EAA or PID by proving access and control over cryptographic material linked to the (Q)EAA or PID" indicates that PIDs allow for online authentication making the difference with (Q)EAA unclear. It would be advisable to make that more clear. Also, how does a PID relate to the eIDAS update proposal itself?
3. In Footnote 15 (page 17) of the ARF it is stated: "Mutual authentication between wallets and relying parties should not be understood as mandatory for every transaction." An example would be helpful here as I have no idea what is meant here. Authentication of the relying party to user seems mandatory to me as otherwise users are susceptible to phishing. This perhaps relates to the PID discussion started above.
4. In ARF Sections 4.6.1 "User awareness component" and 4.6.2 "User authorization mechanism" the fundamental role of user consent (called reliable user confirmation in my Issue #5) is finally identified; it is lacking in the eIDAS regulation itself. What is lacking however is the level of assurance in which consent shall be implemented by the eIDAS wallet. As I argued in Issue #5 such consent is so security vital in authentication that it also should protect against attackers with 'high attack potential', i.e. the security level of the eIDAS wallet authentication mechanism itself. For instance, I don't think you want such consent to be implemented in an internet

browser as then man-in-the-browser malware can fool you and let you sent sensitive data to the parties you are not aware of. That is the classical modus operandi so successfully used in internet banking fraud.

5. In ARF Section 4.8.3 “Interface towards relying parties, brokers or proxies” the role of proxies is addressed, i.e. parties sitting between the user and the relying parties providing support to the relying parties. This section only states that through the use of proxies “the reliability of the authentication mechanism shall not be affected.”. As indicated in my Issue #9 also the confidentiality of the attributes traveling through the proxy shall not be affected. That is, to protect the user privacy the proxy shall not have access to the plaintext attributes. I also sketched how Issue #9 can be easily implemented through the use of QR-codes.