QUALI-SIGN AND SGM CONSULTING COMMENTS ON ARCHITECTURE AND REFERENCE FRAMEWORK (ARF) DOCUMENT

Section 4.1 Store person identification data… & Section 4.4 Mutual authentication: Offline connectivity and storage interface for EUDIWs

We support the emphasis put on offline connectivity for EUDIWs, which is needed for many use cases, and certainly critical for POS payment authorization interactions. In particular we appreciate the wording of section 4.4 Mutual authentication.

We note, however, that footnote 15 mentions that mutual authentication may not be always required but fail to understand why this should be the case given that it does not affect the customer experience nor does it imply additional costs. We only see benefits and no downsides in having mutual authentication performed for each and every interaction between EUDIWs and relying parties.

Given the focus on offline connectivity – which we fully support – we fail to understand how the EUDI Wallet storage can be meaningfully ‘remote (in a cloud-based infrastructure)’ as a self-sufficient alternative mentioned in the second paragraph of section 4.1. The related footnote 12 mentions ‘additional challenges’ in this context. To put it directly, we do not see how this could work (particularly when both the relying party and wallet are offline) and would welcome clarifications on this aspect.

Indeed, local storage using X509 certificates applying ETSI standards (notably 119 411-2) for PIDs and (Q)EAAs pointing to the wallet identity certificate (itself linked to the secure element of the smartphone) allows a secure management of identity and other attributes which can be communicated online and offline. This allows online and offline client authentication for all interactions with relying parties, root of trust verification of all certificates as well as mutual (wallet user/relying party) consent whenever needed – a essential requirement for the payment authorisation use case where legal irrevocability needs to be established.

(link to graphic description of the wallet local storage: https://sgmconsultingservices.com/wpcontent/uploads/2022/04/Image1.png)

Section 4.5.1 Offline sharing

The section contemplates a scenario where a physical ID document with biometric data is required to be presented for identity-proofing purposes of the wallet user, a situation resulting from the fact that the electronic attestation is ‘not linked to the EUDI wallet’. This situation should simply not be allowed and all attestations should be linked to the EUDI wallet, and therefore the wallet user. Indeed, the link should be required irrespective of whether they are PID, QEAA or mere EAA attestations. In short, we see no rationale at all for ‘unlinked’ attestations. This can only weaken the trust put into EUDI wallets.

section 4.8.2: Interface towards Member States identity cards – treatment of facial image as an attribute

We note, in line with other contributors, that EU regulation 2019/1157 drastically restricts access to ‘biometric data stored in the storage medium of identity cards and residence documents’ (including the facial image), which ‘shallonly be used by duly authorized staff of competent national authorities and Union agencies for the purpose of verifying (a) the authenticity of the identity card or residence document and (b) the identity of the holder […] where required to be produced by law’ (article 11.6). We wonder if the initial identity-proofing (binding) process implemented by providers of PID can achieve a high LoA when they are legally prevented from having access to the facial image of the holder in the card chip.

We recognise however that, as directed by GDPR requirements for biometric data, the facial image warrants enhanced protection, and would suggest either prohibiting it from being an identity attribute transferable to any relying parties – indeed this is not needed to ascertain that the person it the wallet's legitimate user – or restricting its communication to those relying parties that have a legitimate interest, such as, for example, police and customs officers. At a technical level, this can be done by requiring the relying party to first present to the wallet a dedicated electronic attestation showing that it is entitled to request the facial image (or other biometric data), meaning that no communication would be possible unless this attestation is first presented to the wallet. This can be simply achieved with X509 attribute certificates meeting ETSI standards. In our opinion, it would be beneficial to extend this approach to other 'privacy-sensitive' attributes, such as the unique identifier – see below.

Export of EUDI wallet interaction history for dispute resolution purposes and compliance with regulatory requirements

We are very supportive of the requirement for the EUDI Wallet to provide the user with access to the history of their digital identity transactions (see articles 4.6.1 and 5). However, we suggest that the text be extended to explicitly state that the EUDI wallet user is always entitled to export a copy of the digital identity proof (incl. Qualified Signature) created during interactions with relying parties. The user would then be able to present this as evidence, including for compliance with regulatory requirements and court proceedings. All use cases are relevant here, but this is especially relevant for payment authorisations.

Legal person wallets / Identity Profiles

We believe it is important for EUDI wallet users to be able to segregate their personal and other identity profiles (e.g., a natural person authorized to act on behalf of a legal person) within the wallet. Otherwise, requests are likely to be made to install multiple wallets on the same device in order to achieve this segregation.

With respect to export of the wallet interaction history mentioned above, we believe it is appropriate for the legal person (e.g. the employer) to be able to restrict the representative user's ability to export the proof (of potentially sensitive business-related digital identity transactions) to their personal device. Instead, the legal person must have the ability to export the proof in a secure manner and also have access to the history.

COMMENTS RELATED TO THE EIDAS 2.0 DRAFT PROPOSAL.

Article 11a of draft eIDAS 2.0 proposal: Privacy protection and 'Unique and Persistent Identifier'

The ARF, and indeed the draft eIDAS 2.0 proposal, rightly emphasise the need to protect privacy, which includes ensuring that no relying party should be allowed, or indeed able, to trace the use of EUDIWs. On the other hand, we also understand the need for certain public authorities – e.g. tax authorities - to have access to a unique identifier as set out in article 11a of the draft eIDAS 2.0 proposal.

As for the facial image discussed above, an efficient way to reconcile the two requirements would be to have those relying parties authorized to request the unique identifier present a dedicated electronic attestation to this effect, which would result in no communication of the unique and persistent identifier being possible unless this attestation is first presented.

Article 6.bof draft eIDAS 2.0 proposal: EUDI Wallet relying parties

We are really puzzled by article 6b, especially when requiring all relying parties to 'communicate to their member States their intention to rely on EUDI wallets and informing about the intended use of EUDI Wallets' (article 6b1). We see no clear rationale for this requirement and fear this will prevent the deployment of fully legitimate use cases for EUDI Wallets, especially for SMEs, professionals and indeed individuals who should be able to act as relying parties. Also, does this imply that non EEA/EU relying parties – who have no 'member State' – cannot rely on EUDI wallets? It strikes us that this is a major deviation from what happens in face-to-face interactions when presenting verified ID credentials, such as passports or ID cards. To take a simple example, a licenced liquor merchant does not 'notify' its member State that it is to accept national ID cards or passports to check that customers are over 18 years old.

To address this, one possible option could be to differentiate between certified relying parties (who have communicated their intention to member states) and two EUDI wallet users who wish to bilaterally conduct a digital identity transaction between their two wallets. In the latter case, we suggest that both users should be required to perform Strong User Authentication on the transaction. This approach would be applicable to P2P transactions between two wallets.

With respect to the 'common mechanism for the authentication of relying parties' (Article 6b2), we suggest that whenever relying parties (other EUDI wallets, terminals, websites etc) initiate a EUDI wallet based digital identity transaction, they must include a specific attribute attestation within their request. This attribute would include the name of the relying party, which can then be displayed by the receiving EUDI wallet to their user. Michael ADAMS/Quali-Sign

Stéphane MOUY/SGM Consulting

Michael Adams and Stéphane Mouy are both members of the eWallet Network