eIDAS Architecture Reference Framework 1.0 – comments and first analysis

12. February 2023

Authors: Thomas Lohninger and Kai Wagner

Timing and Influence on the Negotiations

The Architecture Reference Framework (ARF)[1] was scheduled to be released four months ago. Earlier versions were rejected by member states on the grounds of being incomplete and not detailed enough to base the eIDAS large pilots onto them. The document that was now released already circulated in adjacent bodies to the expert group whereby being available to vendors and government official since mid January. Further comments from academia, civil society or the public were not invited. The release of this document on the day after the ITRE vote seems to be very intentionally timed.

The document stays silent on many of the architectural safeguards that the European Parliament has adopted in committee stage. While it explicitly only referred to the Commission proposal and states that the legislative process will be reflected in subsequent versions of the ARF, several design decisions it already outlines are incompatible with safeguards adopted by Parliament and Council.

The biggest risk for negotiators should be that in the soon to start trialog negotiations are confronted with arguments around technical feasibility that are not neutral, but vendor and surveillance interests driven. It appears to be at least inefficient, if not undemocratic to establish a technical architecture on a law that is still under negotiation.

Unique Persistent Identifiers through the Backdoor

The ARF proposal does not establish a clear foundation for how pairwise pseudonymous interactions can be enforced. Practically, the current model relies on a setup where in each and every interaction the same public key is exchanged, which is a privacy nightmare, since it is a unique identifier that is shared with everyone all the time. This foundational privacy issue needs to be addressed in order to ensure that this solution can be privacy by design and even GDPR compliant.

Even if the European Digital Identity Wallet (Wallet) were to be privacy-respecting in its other functions to exchange information, the current architecture can be seen as relying on a "super cookie" in the form of a public key that allows tracking of every single user interaction across all relying parties.

In light of the lengthy political discussion about unique, persistent identifiers in Article 11a it seems improper to reinsert a unique, persistent identifier on a low technical level that circumvents the safeguards introduced in Article 11a by both Parliament and Council.

The design choices reflected in the ARF are not without alternative. There are more privacy preserving solutions developed in the open source community, that are not even discussed.[2] Privacy by design is

1 https://ec.europa.eu/commission/presscorner/detail/en/mex_23_765

2 such as "linked secret" based binding as found in https://hyperledger.github.io/anoncreds-spec/ or privacy preserving signatures like BBS+ https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html

an integral part of all modern authentication protocols such as FIDO U2F and FIDO2 where it is clearly defined that no unique key or identifier is used. Each interaction is split at least into relying party specific keys.

The Risk of "Over-Identification" is still Unmitigated

Also, there should not be the notion that we should identify everyone all the time. Providing a Wallet with government certified personal data via a universal interface creates an incentive for relying parties to over-identify currently anonymous or pseudonymous use cases or require data from users/customers they only ask for because of the convenience of the Wallet. We have warned about this risk from the beginning[3]. The Wallet brings this huge risk, which needs to be safeguarded against, as also mentioned by the EDPS Wojtek Wiewiorowski.[4]

Still Missing: Preventions against Fraud, Identity Theft and GDPR Violations

While chapter 6.2 on the trust model mentions "Relying Parties' registration and authentication." as a todo for subsequent versions of the ARF, this section will only be useful if the Regulation maintains proper requirements for safeguards on registration and revocation of relying parties. In both the Council and Parliament versions of the text we can find rules about bad and fraudulent relying parties being revoked their right to rely on the Wallet. There was also legal language that would restrict the Wallet to only allow the relying party to ask the user for information according to accepted and registered use-cases. Right now, this is not certain and this single todo line is the only reference to such a mechanism in the ARF. The technical support for strong safeguards (something along the lines of authorization certificates for relying parties) would be easy to do, but is still missing. Industry is lobbying very hard to prevent such safeguards against abuse, with the argument that it might hinder rollout of the new system.

Security pragmatism with Levels of Assurance (LoA)

A hotly debated question is the Level of Assurance (LoA) for the Wallet. Both Council and Parliament spent a lot of time debating this question. The decision was made that LoA high is the foundation of the Wallet, that is good in so far as this ensures highest security in identity proofing. Still, requiring all attestations in the wallet to be provided on LoA high would be too complex and simply uneconomical for many lower-level attestations such a for example train tickets.

To mitigate this adoption risk, we see a differential security approach described in 6.5.2 and 6.5.3 where two types on configurations are described that enable more flexibility to attestation providers. Finally, for simple Electronic Attribute Attestations (EAA) such as a theatre ticket or voucher, there is no Level of Assurance required.

Many Member States will have to start from scratch

The PID Dataset (eID part) in the Wallet is supposed to be modeled based on the same technical framework as QEAA's, effectively, the PID dataset is just one well defined instance of a QEAA. This is a major difference to today's model, where national eID systems are highly different in their technical makeup.

3 https://en.epicenter.works/document/3865
4 https://edps.europa.eu/system/files/2023-02/23-02-07_ww-enisa_en_2.pdf

This will likely be one of the biggest points for discussion, since it effectively means that governments cannot use their existing eID system anymore. Also, the LoA high requirement will require some member states with established systems based on LoA substantial to start from scratch.

We already see Italian players lobby against this in full force.[5]

We might still need Hardware Tokens or we would leave many People behind

Reliance on Secure Element storage for private keys and similar core functions of the Wallet is a good thing, still, this is highly experimental today and we might thus see that many states will instead require to use the Wallet in combination with eID cards as a hardware token or something alike in the first years, simply because the tech for embedded security on LoA high is not available in most devices.

As a compromise Secure Elements could be offered in different external form factors, such as existing write-locked and non-extensible eID cards. Well-known examples are citizen or tourist cards, company IDs, health insurance IDs, payment cards, signature cards or wearables combining any or all of those options. The secure chips inside those cards mostly satisfy the requirements for LoA high.

There is a Kill-Switch on the Wallet for Member States

The fact that member states have the power to suspend the full Wallet and the PID and stop it from functioning is problematic. Suspension rights should only be possible for those components that are attested by the Government. So for example not for EAA's of university diplomas or airline tickets, they should remain usable even if the PID dataset was revoked or a Wallet was suspended.

Chapter 4.2.4 hints into that direction but we will have to see if that will be possible in the actual implementation.

Control over the Wallet will not be with the User

It is interesting that the ARF mentions that citizens could have full control over their private keys via the Cryptographic Keys Management System, but that control will be limited, since the hardware security modules can only be accessed via mediators[6] and often the Smartphone vendors simply don't allow full access to the contents of the secure systems.

So here, we should not expect full control which renders the central promise of the Wallet mute. It would also run contrary to the rights under the GDPR for data portability to switch from one Wallet to another. In practice, a lot will be determined by how key revocation and backup processes are established and whether they are protecting the user well against misuse by the state or the Wallet issuer. The ultimate question is whether this key management system will be privacy by design, thus protecting the user from the parties that provide it to her in the first place.

Technical Feasibility of the Architecture tries to be Everything for Everyone

The dual issuance of attestations (PID and QEAA) is an interesting choice and mainly done in order to support both digital interactions and offline onsite proximity interactions well. The practical challenges

5 https://blog.quintarelli.it/2023/02/an-upcoming-major-blow-to-eu-digital-identity/

6 Such as eg. the Trusted Service Management System service that is used to provision the secure element in case of the German Smart eID Secure element applet https://github.com/BSI-Bund/TSMS

of that are that W3C Verifiable Credentials have a different Trust Architecture than ISO mDocs and now, the Wallet, as well as the issuer and verifiers all need to support both. This double work might result in a weird architecture, but it is the only way the requirements (support for the 4 types of presentation flows in chapter 6.4) from the eIDAS regulation can be met with today's technology.

PID and QEAA differ almost only in the issuance MUST requirements. For PID, it is left to the national issuing bodies (which can be the same as the Wallet providers) and for QEAA it specifies the OIDC for Credential Issuance protocol.

The Wallet still tries to satisfy too many use cases for too many stakeholder groups without having consensus among the member state from even being used instead of existing national systems. A separation of use cases in tiers for certain groups of use cases would be the easier, cheaper and safer option.

Conclusion

On the one hand the ARF is too little too late. On the other hand, one could argue that the whole process should never have started before the legal basis is democratically agreed. The risk of this document being abused in negotiations to force MEPs to agree to Commission demands remains high.

The original outline for the eIDAS ARF from February 2022 includes principles like "un-traceability" and "unlinkability".[7] These important privacy-preserving principles have sadly been removed from the ARF 1.0. Contrary to what the Commission might think, the success of the Wallet will not depend on the many compliance certifications that are foreseen in the legal proposal, but on the level of trust normal citizens will place in this system to handle their sensitive data securely and privacy-respecting. If trust is the goal, the Commission is doing everything wrong to get us there.

7 https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline