4th LIBE Shadows meeting on eIDAS – 22-03-2022

Prof. dr. Eric Verheul, Radboud university

Slides available at my personal Radboud page.

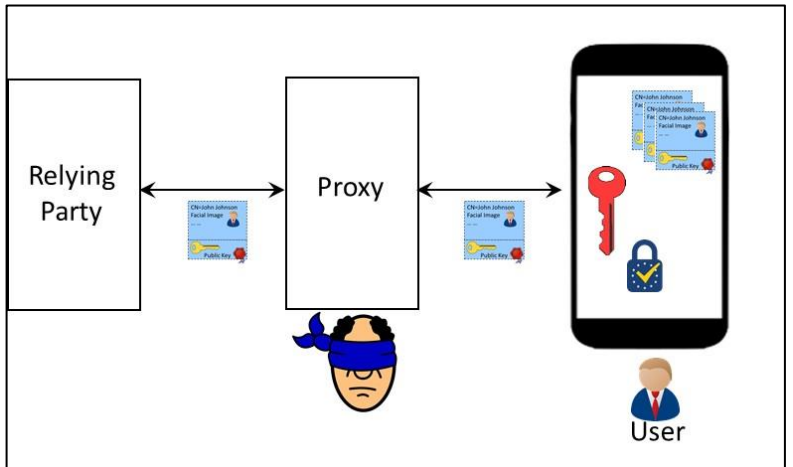
Outline

- Some observations on Architecture and Reference Framework (ARF)
- Answering the three EPP questions posed
- Conclusion

Some observations on ARF

1. Positive: ARF hints on using existing mobile crypto hardware (TEEs) as basis for eIDAS wallet security. Good news; allows wallets availability for virtually all EU citizens!
2. Negative: Still no clarity on ‘resistance to attack potential’ notion introduced but not defined in eIDAS or its update.
3. Positive: ARF acknowledges the security/privacy relevance of reliable user ‘consent’, unlike eIDAS and its update. However, strength of mechanism is lacking. Should be resistant to ‘high attack potential’!
4. Negative: ARF mentions proxies sitting between wallets and relying parties but does not stipulate security/privacy requirements. ARF should require proxies to be ‘blind’!

Als see https://www.cs.ru.nl/E.Verheul/papers/eIDAS/Some%20observations%20and%20questions%20on%20the%20eIDAS%20wallet%20ARF.pdf



Q1: Tracking by ‘big tech’ of eIDAS wallet

Q1: If we look at the potential building blocks of the wallet in chapter six, we see three possible options: a mobile application, a web application and a secure application on pc. This means that we will need to rely on companies as Apple or Microsoft for their cooperation. How will this cooperation work, will they have any possibilities to track the use of the wallet when used on a mobile app on their devices?

- Not a big concern as Apple, Microsoft and Google allow for independent software development through Software Development Kits (SDKs).
- If we stipulate the use of ‘secure elements’ we could become too dependent on a few parties owning these ‘secure elements’. I don’t think ‘secure elements’ should be mandatory.

Q2: Local or remote storage of eIDAS attributes

Q2: The outline repeats that the storage of the EUDI Wallet can be done locally (located on a device the user holds) or remotely (in a cloud-based infrastructure). What is the safest option in terms of data protection in your view? Storing data on each user's device locally has long been seen as the safer option by data protection experts, should we not exclude the option of remote storage?

- We should **not** exclude the option of remote storage but require that attributes are **always encrypted** when stored in 'rest', i.e. either in local or remote storage.
- The crux is then **where** the decryption keys are stored. Keys could also be stored locally (Secure Element) or at a 'wallet service provider'.
- Storing **both** attributes and the keys in the wallet is **not** the data protection safest option as the user can then never be sure his/her personal data is not compromised when his/her mobile device is stolen or lost.
- Storing **both** the encrypted attributes and the keys remotely will allow for easy **recovery** when the user has lost his mobile device or bought a new one. My personal preference!

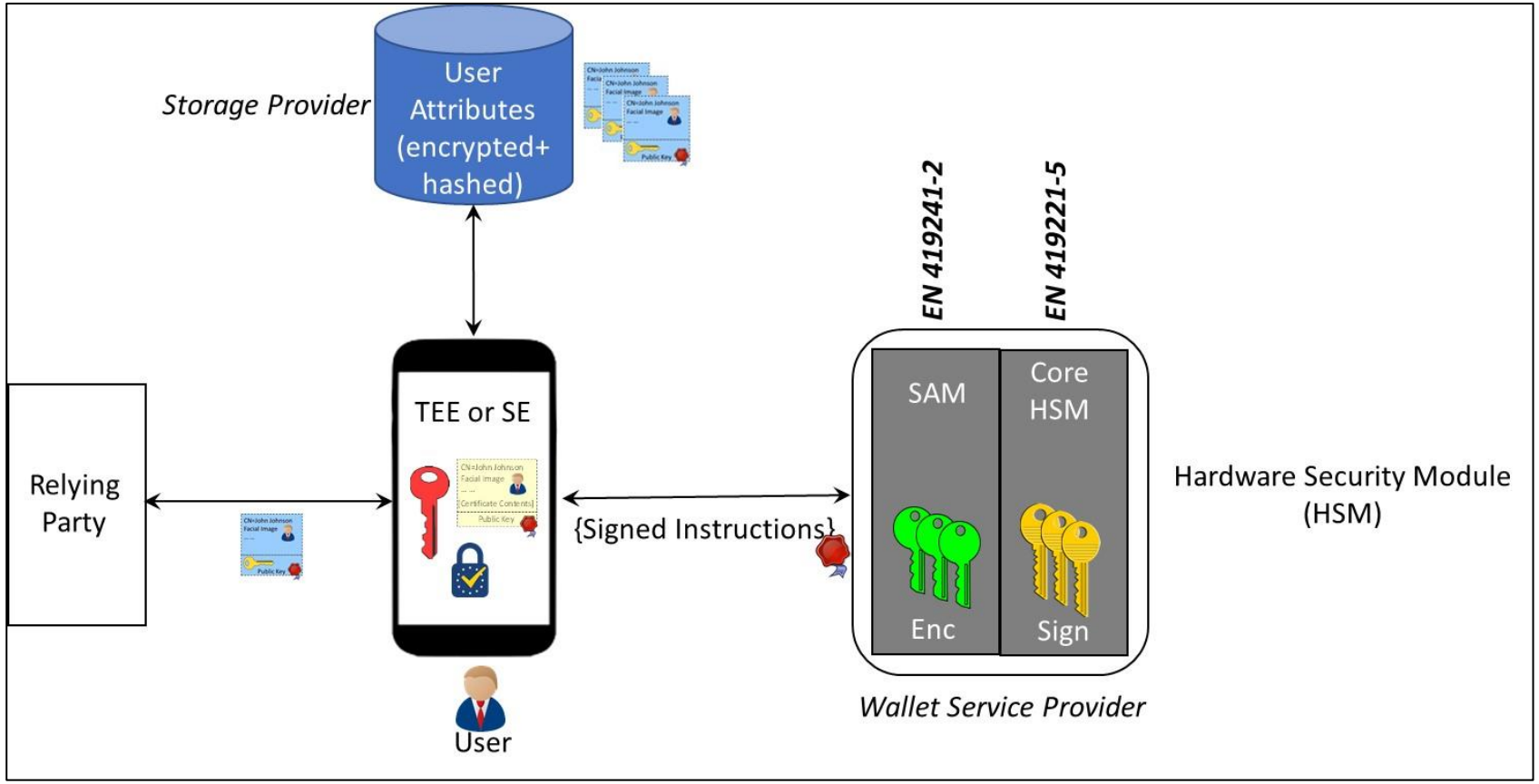
Q3: Optimal use of cryptography

- *Q3: Chapter 4.3 deals with encryption. How do you see the role of encryption in order to ensure the highest level of data protection?*

- **Encryption** of attributes either in local or remote storage
- **Hashing** of personal data in attributes to cater for selective disclosure
- Support of a **variety of electronic signatures schemes**: conventional ones (RSA, ECDSA) but also privacy-friendly ones like CL-Signatures and quantum computer proof signature schemes.
- Decryption/signature keys:
  A. stored in a '**Secure Element**' in mobile device, or
  B. stored in a Hardware Security Module at 'wallet service provider'; access controlled by user based on one cryptographic key stored in **TEE or Secure Element**. EU regulation same as with qualified remote signing.

- Option B is my personal preference.

Conclusion



- Don’t only look at ‘data protection’ but also consider trade-off with security and user-friendliness
- Give EU citizens enough room to make their own choices, otherwise the wallet will not be successful