

eIDAS: LIBE Shadow Meeting

Thomas Lohninger (epicenter.works / EDRI)

Brussels/Internet, 9. February 2022



MISSING SAFEGUARDS

trust is hard earned and easily lost

Unobservability

Artike 6a (7)


[...] The issuer of the European Digital Identity Wallet shall not obtain~~collect~~ information about the use of the wallet [...].

Regulation of Relying Parties / Use-Cases

- eIDAS regulator approves use-cases ex-ante, potentially require DPIA
- Blacklist of prohibited use-cases (advertisement, financial scoring and real name policies on social media platforms)
- Complaint procedure with national regulator to remove relying party (data & consumer protection, IT-security breaches, dark patterns, etc.)
- Missing: Privileges what information relying party can obtain from user
(Wallet needs to know what relying party is allowed to ask for)

Unlinkability

- Remove Article 11a!
- Define Selective Disclosures meaningful (fix Article 6a(4)(d) & 3(5))
- Any (alphanumeric) identifier has to be specific per relying party (***otherwise we invite tracking, see NIST SP 800-63C***)



OPEN QUESTIONS

Also we need to fix...

Relationship to GDPR?

Article 5

Data processing and protection Pseudonyms in electronic transaction

- ~~1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.~~

Article 12

Cooperation and interoperability

3. The interoperability framework shall meet the following criteria:

~~(d) it facilitates the implementation of privacy by design; and~~

~~(e) (d) it ensures that personal data is processed in accordance with Directive 95/46/EC~~

Who is the Controller?

*'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means** of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, **the controller or the specific criteria for its nomination may be provided for by Union or Member State law;***

– Article 4 (7) GDPR

Provider of the European Digital Identity Wallet should be the Controller

See also Case Jehovan todistajat C-25/17

Other Issues

- What does the Wallet need to show the user for informed consent?
- Is it still free consent, if Government services cost more without eID?
- Storage of Biometrics in the Cloud? (Recital 11)
- Article 20(2): Data Breaches need to be notified to the Controller & Data Subject
- Article 48a should include other risks as reporting obligation
- Remove Article 45!