eIDAS: LIBE Shadow Meeting

Thomas Lohninger (epicenter.works / EDRi)

Brussels/Internet, 22. March 2022

1

ASSESSMENT OF RAF OUTLINE

eIDAS Expert Group Reference Architecture Framework Outline: Feb 2022

Unobservability

The EUDI Wallet **shall** make it impossible to collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it.

– Section 4.5

Cloud Wallets

*“The EUDI Wallet shall have either only a local storage, or **a hybrid storage with at least pointers to a remote storage** which are stored locally. “*

– Section 4.1

*“Form factors:
*

Form factor 1: Mobile application
*Form factor 2: **Web application***
Form factor 3: Secure Application on PC“

– Section 6

Regulation of Relying Parties / Use-Cases

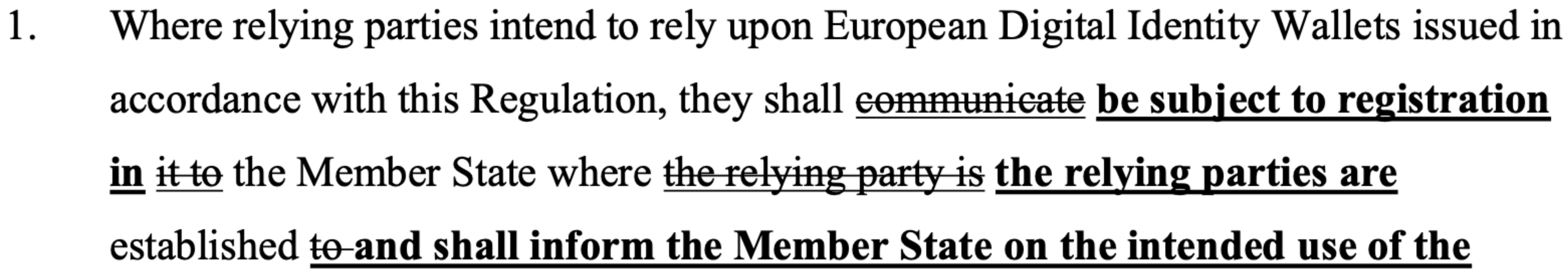
*“To ensure informed actions from the user and adequate security levels, the EUDI Wallet […] **shall be able to identify and authenticate the third party it is interacting with.**“*

– Section 4.4

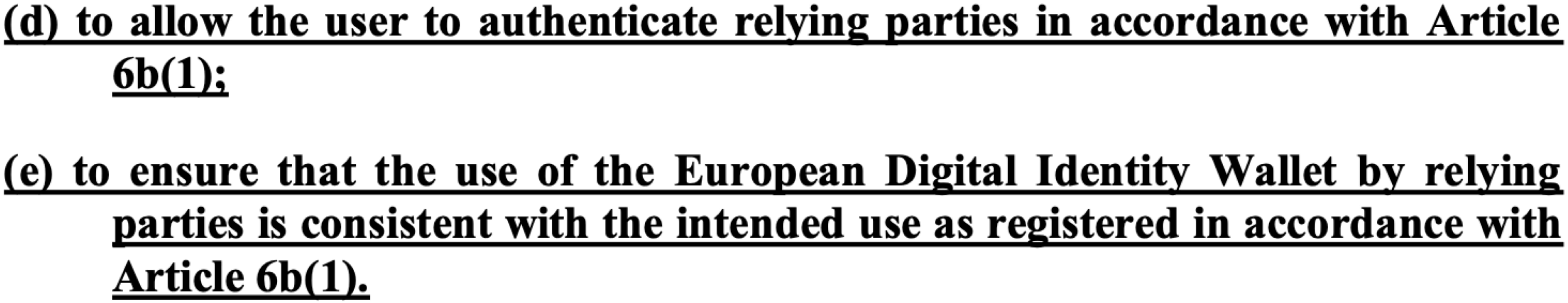
*“In addition, the EUDI Wallet may: […] **restrict sharing certain sets of attributes with certain parties**, or warn the user that the relying party may not be authorized to use/ask for these attributes.“*

– Section 4.6.1

Regulation of Relying Parties / Use-Cases



1. Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall ~~communicate~~ **be subject to registration in** ~~it to~~ the Member State where ~~the relying party is~~ **the relying parties are** established ~~to~~ **and shall inform the Member State on the intended use of the**



(d) to allow the user to authenticate relying parties in accordance with Article 6b(1);

(e) to ensure that the use of the European Digital Identity Wallet by relying parties is consistent with the intended use as registered in accordance with Article 6b(1).

– Article 6a & 6b from French Presidency Compromise (March 10th 2022)

Sounds good, but means little

“The EUDI Wallet shall ***enforce privacy by design*** *and* ***selective disclosure*** *of attributes.“*

– Section 4.5

“The EUDI Wallet shall enable the user to share only the information they intend to share. The Wallet shall ensure an ***appropriate level of privacy****, implementing policies about* ***non-traceability*** *and* ***unlinkability*** *of user’s activities for third parties as appropriate considering:*

- *the applicable legal context for identity providers and* ***attestation providers****;*
- *the need to retain evidence for* ***dispute resolution purpose****;*
- *the* ***right for the user to be informed of the use of their EUDI Wallet****. ”*

– Section 5

Potentially dangerous Loophole

“Selective disclosure and combination of attestations can be handled in two different ways:

- *the EUDI Wallet may hold a very broad collection of attributes as PID, QEAA and EAA, and **each time a specific attribute or the derivation of a specific attribute is required, a new PID or (Q)EAA has to be requested from providers**.*

- *The EUDI Wallet may have the intrinsic capability, based on the obtained PID and (Q)EAA, to selectively disclose, derivate a specific attribute and aggregate several single attributes, without the need for new PID, (Q)EAA or interactions with the PID and (Q)EAA providers. For instance, specific fit for purpose signature schemes in PID and (Q)EAA could enable such capabilities. ”*

– Section 4.6.1

Conclusion

- Many details are missing
- Central requirements not yet implemented, e.g.: privacy by design
- Dodged big questions (virtual wallet, toxic use-cases, circumvention of EUDIW safeguards by data portability, etc.)
- Expert Group ≈ Council. follows co-decision, legislator leads!

Q&A

Thanks EPP

Question 1

*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?*

Question 2

*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**?*

Question 3

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