German Banking Industry Committee

Die Deutsche Kreditwirtschaft

German Banking Industry Committee contributions to the draft implementing regulation laying down rules for the application of Regulation (EU) No 910/2014 (integrity and core functions, personal identification data and electronic attribute attestations, protocols and interfaces to be supported, certification)

German Lobby Register No R001459
EU Transparency Register No 52646912360-95
Contact:
Tim Kremer
Telefon: +49 30 20225- 5314
Telefax: +49 30 20225- 5345
E-mail: tim.kremer@dsgv.de

Berlin, September 25, 2024

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

I. In General:

We are thankful for the opportunity to comment. In this paper, we provide some basic considerations and additional suggestions.

The Implementing Acts are too general overall. It must be ensured that Europe-wide technical and legal interoperability is guaranteed and that the same conditions for the provision and use of the wallet apply throughout Europe. It should be prevented that so-called technical and legal intermediaries ('converters') become necessary between the countries. In particular, there must be no so-called 'gold-plating', whereby stricter requirements apply in one member state than in another.

The drafts for the Implementing Acts are recognisably unfinished. They need to be more specific and contain essential requirements directly, e.g. parts of the ARF could be transferred to the Implementing Acts. The ARF already uses established terms, definitions and technical descriptions that are not reflected in the current drafts. For example, the term 'Wallet Secure Cryptographic Device' (WSCD), which is defined in every EUDIW Implementing Act, should be clarified to the effect that the WSCD can be implemented as a Remote WSCD, Local External WSCD or Local WSCD.

In addition, the European standardisation organisations CEN TC/224 and ETSI ESI are working together to develop a set of standards to support the eIDAS2 legal framework in general and the EU Digital Identity Wallet in particular. The legislative process to develop the EUDIW-IAs should take this standardisation work into account.

Coordinator:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

II. Integrity and Core Functions

- An EU-wide standard is particularly necessary for technical interoperability and is also the basis for the acceptance and dissemination of EUDI wallets.

- The core functions must be described in more detail. For example, it is not clear what it actually means that the mechanisms for the

authentication of wallet users in Art. 6 para. 3 d should be independent of the wallet units; see Art. 6 para. 3 e.

- It should be possible to differentiate between the transaction logs depending on the use case: It will not always be desirable for all transaction logs to be available with all information. This is where the optional version to be set by the user comes in handy. In the same way, there may be use cases in which a complete log should be mandatory. Two examples:

  - For data protection reasons, a natural person decides that they do not want to log everything. They are aware of the risks (data recovery not possible).
  - In case of an organisational wallet, all logs should be recorded and available - by all legal representatives.

- Very different options for creating a Qualified Electronic Signature are still being presented. This presumably reflects the current state of work. It would be desirable if specifications could be provided in a timely manner.

III. Protocols and Interfaces

- The protocols and interfaces are insufficiently described for an implementation to be based on them. They should be better synchronised with the ARF. Uniform technical standards are a basic prerequisite for implementation and are therefore mandatory to define. Standards should avoid variants and options as far as possible to ensure the best possible compatibility.

- The annexes refer to ISO/IEC 18013-5:2021 and W3C Verifiable Credential Data Model. However, issuing protocols such as OpenID4VCI are missing. Here too, the Implementing Acts should be better synchronised with the ARF.

- It is recommended that the Implemeting Acts and the corresponding annex be organised according to the ecosystem presented in the ARF. In addition, the draft standard ETSI TS 119 462 'Wallet interfaces for trust services and signing' can be taken into account with regard to the APIs and protocols to be used for the various types of interfaces.

- For interoperability, at least the following technologies should be considered in practice (QR code, NFC, Bluetooth, data protocols such as interprotocols). Here too, the Implementing Acts should be better synchronised with the ARF.

- The protocols and interfaces should be compatible with or reference other major EU/ECB tech initiatives, e.g. the Digital Euro, to ensure a harmonised digital ecosystem.

- In addition, the draft raises further questions:

  - It is envisaged that further protocols and interfaces can be used for specific use cases, without describing the use cases in more detail.

- It is not clear who the providers of wallet relying party access certificates will be. These must also be certified themselves.

- Not every Relying Party can potentially receive/request every credential, but the publisher determines which group of Relying Parties may read/receive their credentials. This makes sense on the one hand, but on the other hand it increases the complexity of implementation and contradicts the self-sovereign approach. An analogue document does not have this restriction.

- Which protocol should be used to transmit requests for data deletion to Relying Parties?

- In which cases would it not be necessary or applicable to indicate which information (attributes) the Relying Party requires?

- What if the wallet is exchanged for a different wallet? In this case, the new wallet could not be used to ask a Relying Party to delete the data previously shared (with the old wallet)? How should this be handled if this is the intention of the privacy feature?

- For example, if a German wallet is used, would the user inform the German authorities about a misbehaving Relying Party, even if the Relying Party is from another member state? How should the authorities' back-end processes work and what will be the outcome of such a notification? Is this determined at EU level?

IV. Certification

- The individual certification schemes and supervisory bodies are not sufficiently harmonised. There is therefore no standardised Europe-wide level playing field for the certification schemes.

- The EUDIW certification recommendations in the ARF and the EUDIW certification analysis report published by ENISA should be taken into account when developing the Implementing Acts.

- There is no common reliability in terms of data protection compliance. Optional data protection certification for Member States would lead to different levels of data protection.

- A standardised examination of the functionalities and requirements (data sets, etc.) across all certified wallets or all certification schemes is not evident from the current Implementing Acts. The eIDAS Regulation provides for acceptance obligations for certain use cases and sectors. With regard to these, a conclusive and clear definition of the use cases covered by this would be desirable - in a suitable place - or a reference to the relevant place where these aspects are regulated. This is also because further requirements (can) build on these, e.g. in the case of applicable retention periods (see Art. 18 para. 1 of the Implementing Act in the draft 'laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets' with reference to national law or EU legal acts regarding relevant retention periods.

- How would wallet users know if the certification authorities immediately suspend a wallet's certificate of compliance after a security breach or compromise of the wallet affects its compliance with the requirements of national certification schemes? And how are they informed of an imminent cancellation of the certificate of conformity?