

Comments

on the draft implementing regulations on the European Digital Identity Wallets

Berlin, 5 March 2025

Contact:

Diana Campar

Telephone: +49 30 1663 1546

E-mail: diana.campar@bdb.de

Diana Campar

Telephone: +49 30 1663 1546

E-mail: diana.campar@bdb.de

16112 – European Digital Identity Wallet: Standards and technical specifications – Amendment to CIR (EU) 2024/2979, 2982, 2977, and 2980

1. Overarching governance aspects

- **Detailed technical specifications** (e.g., API parameters or protocol details) should not be permanently anchored in CIR annexes if possible, as these change regularly, giving rise to maintenance and interoperability risks.
- Preference should be given to referencing **ETSI, CEN, or ISO standards** as soon as they are finally published. The annex text should only serve as a temporary solution.
- **Versioning** should be designed in such a way that controlled further development remains possible and no unnecessarily rigid version pinning logic arises.

2. Specific points

CIR (EU) 2024/2979

- **Annex III (WIA/WUA):** The content is highly technical and iterative. The detailed specification should be transferred to an ETSI deliverable on the wallet unit or instance attestation and then referenced in the CIR.
- **Annex IV (changes to ETSI TS 119 461 v2.1.1):** Changes should be fed in via ETSI ESI and integrated into the planned update of ETSI EN 319 461. The CIR reference should then be updated.
- **Annex IV (Identity Proofing):** The term “peer reviewed” is not defined in eIDAS/eIDAS2 and should therefore be deleted. Instead, conformity assessment or scheme requirements should be used.
- **Annex V (Amendments to ETSI TS 119 472-1 v1.1.1):** Adjustments should also be integrated into ETSI EN 319 472-1 via ETSI and then referenced in the CIR.
- **Annex XI (Trust Mark Specifications):** No static detailed specifications should be laid down in the CIR. Alignment with the ETSI work and corresponding referencing is preferred.

CIR (EU) 2024/2982

- **Annex XIV (“Where appropriate” DC API):** Paragraph 6.2 (General Requirements, GEN-REQ-02) stipulates that wallet-relying parties should also implement the DC API “where appropriate.” However, since only wallet providers and wallet-relying parties are required to implement it and browsers are currently under no obligation to support the DC API, it is unclear how “where appropriate” should be interpreted. In view of the technical implications,

relying parties should retain the freedom to design and choose the extent to which cross-device or browser-to-app flows are enabled with or without the DC API, also taking into account IT security aspects.

- **Annex XIV (Amendments to ETSI TS 119 472-2 v1.1.1):** Proposed amendments should be integrated into the update of ETSI EN 319 472-2 via ETSI before the CIR reference is updated.

CIR (EU) 2024/2977

- **Annex I (photo as mandatory PID element):** The inclusion of a photo as a mandatory element of the PID is welcomed, as this can provide additional security, particularly in face-to-face use cases.
- **Annex I (optional PID table):** The "Nationality" field should also cover statelessness and relevant protection status (where applicable). A corresponding optional field/parameter should be added.

16113 – European Digital Identity Wallet: Registration of Wallet Relying Parties (Update) – Amendment to CIR (EU) 2025/848

- **Pseudonyms/WebAuthn:** The draft extension to Implementing Act (EU) 2025/848 stipulates that relying parties should accept WebAuthn as an authentication mechanism for pseudonyms (Art. 11).¹ At the same time, the Architecture and Reference Framework defines technical data structures and processing standards for PSD2-compliant SCA credentials in the context of the TS12 specification.² It is unclear how the obligation to accept pseudonyms is to be reconciled with the specifications for PSD2-compliant SCA credentials, especially since, according to the explanatory memorandum, the aim of the amendment is to align with the further development of the ARF. It is also unclear how these regulations relate to the Implementing Act, which actually deals with the registration of relying parties.
- **Title/scope consistency:** The focus should be clearly on "Registration of wallet relying parties" and not unnecessarily extended to "Standards/specs" if this is not the primary subject of the regulation.

¹ <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16113-European-Digital-Id%E2%80%A6>

² <https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts12-electronic-payments-SCA-implementation-with-wallet.md>

- **Internal references/legal certainty:** In Annex II (Art. 1 & 2), the deletion of the references to Art. 3 is incomprehensible. Either the reference should be reinstated or the deletion should be explicitly justified.
- **Annex V (Common API National Registers):** The API specification is very detailed and will continue to evolve. It would be better to standardize it via ETSI and then reference it from the CIR.

16114 – European Digital Identity Wallet: Electronic Attestations of Attributes (Update) – Amendment to CIR (EU) 2025/1569

- **Justification for deletions:** Deletions (including Art. 4.1, 4.3, 9.3) should be clearly justified, e.g., in recitals or the explanatory note, to avoid uncertainty for issuers and auditors.
- **Annex I – Scope Discipline / ETSI Baseline Alignment:**
 - **Art. 3(3):** It should be clarified why ETSI TS 119 471 clause 4 should not apply.
Recommendation: Reinstate, unless there is a justified exception.
 - **REQ-EAASP-6.3-02:** The content appears to be a requirement for qualified electronic archiving rather than for EAA issuance. This requirement should be moved to the Archiving CIR.
 - **REQ-EAASP-7.2-02 / 7.2-03 / 7.8-05 / 7.8-07:** These are horizontal baseline topics and belong in ETSI EN 319 401 rather than being duplicated in the EAA Annex.
 - **REQ-EAASP-7.8-06:** This requirement is apparently already covered by ETSI EN 319 401 and TS 119 471 and should therefore be deleted due to redundancy.
- **Terminology:** No new term “secure cryptographic device” should be introduced. Instead, the existing eIDAS terms (WSCD/QSCD) should be used.
- **Cryptographic requirements:** Additional restrictions on the use of (R)QSCD should be linked to harmonized Common Criteria Protection Profiles (e.g. CEN EN 419 211 / 419 221) instead of formulating specific EAA requirements in the annex.
- **Updating standard references:** References to current ETSI versions (e.g., ETSI TS 119 478) should be checked and updated.

Published by:

Bundesverband deutscher Banken e. V.

Burgstraße 28

10178 Berlin

Germany

Lobby Register No R001458

EU Transparency Register No 0764199368-97

USt-IdNo DE201591882

Contact:

bankenverband@bdb.de

bankenverband.de

Responsible for content:

Thematic group Banking Technology and Security

Diana Campar, Associate Director

Diana Campar, Associate Director