FINAL

European Credit Sector Associations (ECSAs) contributions to the draft implementing regulations on the European Digital Identity Wallets

5 March 2026

ECSA eID TF Secretariat: European Associations of Co-operative Banks, Rue de l'Industrie 26-38, B-1040 Brussels
Tel: +32 2 230 11 24, E-mail: chiara.delloro@eacb.coop
Transparency register: *4172526951-19*

Feedback on the Draft Implementing Act amending Commission Implementing Regulations (EU) 2024/2979, 2982, 2977 and 2980 (Art. 5a(23))

The European Credit Sector Associations (European Association for Co-operative Banks, European Banking Federation, and European Savings and Retail Banking Group – ECSAs) e-ID Task Force would like to share observations regarding the draft implementing regulation prepared by the Commission concerning the updated references to standards and technical specifications to ensure that Member States can develop and provide the EUDIW in an interoperable manner.

- **Art. 2(3) new Art. 5a and Annex II (Annex Ia) – Reference to ENISA 'Agreed Cryptographic Mechanisms'**

The draft refers dynamically to the ENISA 'Agreed Cryptographic Mechanisms' without fixed versioning. This may affect legal certainty and foreseeability.

We therefore **recommend** that the **Commission introduce explicit versioning of the referenced document or incorporate the relevant cryptographic parameters directly into the Annex**.

- **Art. 2(4) amending Art. 6**

The amendment to Art. 6 requires that each wallet unit contains wallet instance attestations with public keys and that the corresponding private keys be protected by a wallet secure cryptographic device. This may create hardware dependency and requires assessing the technological feasibility of integration on users' smartphones, taking into account differences between operating systems (e.g., Android and iOS).

- **Art. 2(9) – New Art. 14a on EU Digital Identity Wallet Trust Mark**

Clarification is needed on how this type of certification is structured and what it represents (e.g. security, compliance). It is also necessary to define a clear user experience (UX) to ensure that users understand what is, and is not, certified by the Trust Mark. Clarification is also needed on liability in cases of improper or fraudulent use of the Trust Mark by third parties.

In addition, the **mandatory display of the Trust Mark** and the detailed graphical specifications (including Pantone colours, RGB values and minimum pixel size) appear **overly prescriptive** and may limit technological neutrality and accessibility. We therefore **recommend adopting functional requirements rather than detailed design parameters and ensuring flexibility for future technical environments**.

- **Annex I (general remarks relating to the Anti-Money Laundering Regulation (AMLR))**

Due to the AML-legislation, financial institutions have to collect certain data elements pursuant to the customer due diligence (CDD). The European Banking Authority (EBA) has prepared draft Regulatory Technical Standards relating to this customer due diligence under the AMLR. This draft is currently

followed up upon by the AMLA. For natural persons, the draft RTS indicated that the following mandatory PID are required for the CDD:

Mandatory PID 1. family_name 2. given_name 3. birth_date 4. birth_place 5. nationality
Optional PID: 1. residentaddress 2. resident_country 3. resident_state 4. resident_city 5. resident_postal_code 6. resident_street 7. resident_house_number 8. personal_administrative_number

However, the following PIDs are missing (where applicable):

1. data covering statelessness and refugee or subsidiary protection status (where applicable)
2. tax identification number (if this is different from the personal_administrative_number)
3. a postal address if there is no fixed residential address with legitimate residence

If these data elements cannot be derived from the EUDIW, either as part of the PID or otherwise, financial institutions will need to verify them using other means such as identity documents or other reliable and independent sources. This will lead to the undesirable situation in which customers will still need to provide an identity document, even when onboarding using the EUDIW.

- **Annex I (replacing the Annex to Implementing Regulation (EU) 2024/2977), Table 1 – Mandatory portrait**

We acknowledge that the inclusion of a **portrait** in the set of natural person identification data can facilitate proof-of-presence checks and support both face-to-face and remote onboarding processes. A portrait photo does not in itself constitute biometric data under the GDPR. However, where the portrait is processed through automated means for the purpose of uniquely identifying a person (e.g., facial matching against a selfie), this is likely to constitute biometric data processing within the meaning of Art. 9 GDPR. While the portrait attribute may therefore enhance usability and reduce the need for parallel collection of full ID document copies, a blanket mandatory inclusion for all use cases may raise proportionality and data minimisation concerns, particularly where visual identification is not required. We therefore **recommend that the Commission assess whether the portrait attribute should be context-dependent or subject to selective disclosure and clarify under which conditions automated facial comparison would be permissible, including the appropriate legal basis under the GDPR**.

In additions, some portrait-related tests, such as those on so-called liveness detection tests, should be left to the wallet service provider for security purposes.

- **Annex I (replacing the Annex to Implementing Regulation (EU) 2024/2977), Table 2 – Optional person identification data for the natural person**

We suggest **moving the 'family_name_birth' and 'given_name_birth' data from the optional to the mandatory PID data set**. This would facilitate identity management for people whose common name does not correspond to their birth name, as well as for spouses.

- **Annex I, Table 2 – Personal administrative number**

The inclusion of a personal administrative number may result in a persistent cross-sector identifier at Union level, increasing risks of profiling and undermining the principle of data minimisation.

We therefore **recommend** explicitly **clarifying that no EU-wide unique identifier is created** and reinforcing purpose limitation safeguards.

- **Annex I, Table 2 – Optional inclusion of handwritten signature**

We suggest, where available, the **inclusion of the handwritten signature** present on certain national electronic identity documents (e.g. the CNIe), at least **as an optional person identification data**. This would support banking groups that continue to rely on a copy of the handwritten signature for manual verification checks and help ensure continuity of existing verification processes.

- **Annex III (Annex Ib) – Introduction of the wallet instance attestation (WIA)**

The introduction of the **wallet instance attestation** (WIA) establishes a new mandatory architectural control layer within the EUDI Wallet ecosystem. This measure goes beyond purely technical interoperability specifications and has systemic implications for authentication flows, lifecycle management and operational dependencies. Given its structural relevance, it is not entirely clear whether Art. 5a(23) of Regulation (EU) No 910/2014 provides a sufficient legal basis for such architectural design decisions via implementing act.

We therefore **recommend** that the Commission provides an **explicit legal justification for introducing the WIA under Article 291 TFEU and clarify why this measure qualifies as a purely technical specification**. If necessary, the Commission should consider whether a delegated act would be the more appropriate instrument.

- **Annex III (Annex Ib), TR-WIA-3.1 – Validity period of less than 24 hours**

The requirement that wallet instance attestations must have a time-to-live of less than 24 hours effectively creates a permanent online dependency between wallet units and wallet providers. While this may be intended to mitigate risks related to the security posture of the device on which the wallet operates, this may negatively affect system resilience, scalability and the viability of offline use cases.

We therefore **recommend** that the Commission **provide a detailed security rationale for the 24-hour limitation and assess whether longer or risk-based validity periods could achieve the same security objective** while maintaining system resilience and offline functionality.

- **Annex III (Annex Ib), TR-WP-WIA-3 – Single-use requirement**

The obligation that wallet instance attestations may only be used once could lead to the creation of centralised transaction logs and increase the risk of structural traceability of wallet interactions. This raises questions in relation to the principles of data minimisation and data protection by design under Articles 5 and 25 of Regulation (EU) 2016/679 (GDPR).

We therefore **recommend** that the Commission **assess whether alternative replay protection mechanisms could be used** and clarify that the requirement must not result in systematic transaction monitoring capabilities.

- **Annex III (Annex Ib), LC-WP-WUA-3 – Minimum remaining validity of 31 days**

The obligation for wallet units to always present a wallet unit attestation with at least 31 days of remaining validity may result in recurring synchronisation obligations and increased operational dependency on wallet providers. The necessity of this fixed threshold is not explained in the draft.

We therefore **recommend** that the Commission **reassess the proportionality of this requirement and consider a flexible or risk-based approach**, **supported by clear security justification**.

- **Annex III (Annex Ib), LC-WP-WUA-6 – Record-keeping of attestation associations**

The requirement for wallet providers to maintain records linking wallet units and wallet unit attestations creates a centralised metadata structure. Without **explicit storage limitation periods**, this may raise concerns under Art. 5(1)(e) GDPR.

We therefore **recommend introducing clear retention limits, transparency obligations towards users and exploring decentralized or pseudonymised alternatives**.

- **Annex III (Annex Ib), R-WP-WUA-1.1 – Status lists of at least 10,000 attestations**

The requirement that a status list must contain at least 10,000 attestations 'for privacy reasons' is not supported by an explicit methodological explanation. Without clear justification, this threshold may create unintended market entry barriers for smaller providers.

We therefore **recommend** that the Commission **disclose the underlying privacy rationale and assess whether proportional or scalable alternatives could be introduced**.

- **<u>Annex III (Annex Ib), LC-PAP-WUA-4 – Revocation status checks every 24 hours</u>**

The obligation for providers of person identification data to check revocation status at least every 24 hours where the PID validity exceeds 24 hours creates a permanent online monitoring requirement and a significant operational burden. Furthermore, the allocation of liability in case of delayed or failed checks is not clearly defined.

We therefore **recommend clarifying liability allocation and evaluating whether event-driven or risk-based revocation mechanisms could provide an equivalent level of security** with lower operational impact.

Feedback on the Draft Implementing Act amending Commission Implementing Regulation (EU) 2025/848 on information that wallet-relying parties must provide to the national registers (Art. 5b(11))

The European Credit Sector Associations (European Association for Co-operative Banks, European Banking Federation, and European Savings and Retail Banking Group – ECSAs) e-ID Task Force would like to share observations regarding the draft implementing regulation prepared by the Commission concerning the updates proposed to the information that wallet-relying parties must provide to the national registers, reflecting the evolution of the architecture and reference framework for the EUDIW since the Implementing Regulation was adopted.

- **Art. 1 – New Art. 11 on Acceptance of Pseudonyms by Relying Parties**

Art. 11(1) requires wallet-relying parties to accept WebAuthn as authentication mechanism for pseudonyms. While WebAuthn is a widely recognised standard, mandating a single authentication technology may reduce technological neutrality and limit flexibility for relying parties operating in regulated or specialised environments (e.g., limitations on the usage of the EUDIW for SCA in certain interfaces). In addition, Art. 11(2) requires that pseudonym registration be linked to the presentation of electronic attestations of attributes. The operational and liability implications of this linkage are not clarified, particularly in cases of revocation, misuse or cross-border disputes.

We therefore **recommend** clarifying that WebAuthn constitutes a minimum interoperability baseline rather than an exclusive mechanism, explicitly allowing equivalent authentication solutions and providing clarification on the modalities of the linkage between pseudonym registration and electronic attestations, as well as on the related liability allocation. Clarification should also be provided regarding the compatibility of the use of pseudonyms with the requirements for Strong Customer Authentication (SCA) for online identification, for example to access a payment account online or to initiate electronic payment transactions.

From a financial sector perspective, the introduction of pseudonyms raises additional implementation questions. Based on the APTITUDE work and TS12, banks will need to set up 'Certificates' to allow SCAs under PSD2 and the future PSR. It remains unclear how this new Art. 11 would interact with TS12 and whether financial institutions would be required to introduce additional authentication layers solely to support pseudonyms. More broadly, there is a legal mismatch between the regulatory requirements for SCA and the mandatory acceptance of the EUDIW. Although in the context of the LSP's is has been stated that 'the EUDIW must be accepted for SCA', it is unclear how both the requirements for SCA can be fulfilled and the EUDIW can be accepted.

We therefore recommend clarifying whether the acceptance of pseudonyms should apply across all financial use cases by default or whether it can be assessed on a case-by-case basis. Where pseudonym use is confirmed, further guidance is needed on the level of 'link' to be retained for the certificates.

ECSA eID TF Secretariat: European Associations of Co-operative Banks, Rue de l'Industrie 26-38, B-1040 Brussels
Tel: +32 2 230 11 24, E-mail: chiara.delloro@eacb.coop
Transparency register: *4172526951-19*

- **Annex I – Point 9**

We note that **point 9 of Annex I has not been amended** in the new draft Annex. We regret that no changes have been made in this respect. As currently drafted, point 9 requires us to declare, for each intended use of a given access certificate, the full list of data, including attestations and attributes, with both user-friendly and technical names, attestation types, and associated syntaxes. For the sake of simplification and operational efficiency, **we would have welcomed the possibility to make a single, general declaration covering multiple intended uses** rather than repeating the same information for each use.

- **Annex I – Addition of Point 16 (Association with intermediary)**

The addition of point 16 introduces an explicit association between a wallet-relying party and an intermediary acting on its behalf. While this enhances transparency, it may create ambiguity regarding accountability where the wallet-relying party access certificate is issued to the intermediary rather than directly to the relying party. Without a clear allocation of responsibility, Member States may adopt divergent supervisory approaches, potentially affecting cross-border interoperability and audit consistency.

We therefore **recommend** clarifying **that ultimate responsibility for compliance with Regulation (EU) No 910/2014 remains with the registered wallet-relying party** and establishing harmonised minimum transparency and supervisory rules for intermediary arrangements.

We also note that the draft text does not clearly define what constitutes an intermediary. As a result, we have several questions:

- Does 'intermediary' include external service providers that a bank may use?
- Could it also include an internal entity within a banking group?
- What would be the legal status of these intermediaries vis-à-vis banks?

- **Annex II – Single common API (Public access to registry data)**

Section 2(1)(b) and (c) require that the common API enable any requestor, without prior authentication, to search and request complete lists of registered wallet-relying parties.

While transparency is essential, unrestricted public access to full registry datasets may increase the risk of automated data scraping, profiling of regulated entities and targeted cybersecurity threats. Although Section 2(1)(f) refers to security by design, no specific safeguards are defined.

We therefore recommend introducing minimum safeguards such as rate limiting, abuse detection and monitoring mechanisms, and clarifying whether differentiated access models may be applied for bulk queries.

- **Annex III – Replacement of ETSI EN 319 411-1 with ETSI TS 119 411-8 V1.1.1 (2025-10)**

The replacement of the previous reference standard with ETSI TS 119 411-8 V1.1.1 (2025-10) may create implementation challenges where certification bodies and supervisory authorities have not yet fully aligned with the updated specification. A rapid transition without a defined transitional period may lead to bottlenecks in certification processes.

We therefore **recommend** introducing a clear transitional period and ensuring alignment with national accreditation and supervisory authorities before full applicability.

- **Annex IV – Compliance with ETSI TS 119 475 V1.1.1 (2025-10)**

Requiring wallet-relying party registration certificates, certificate policies and certificate practice statements to comply with ETSI TS 119 475 V1.1.1 introduces additional technical and certification complexity. This may overlap with existing eIDAS trust-service supervision frameworks and create duplicative requirements.

We therefore **recommend** assessing potential overlaps with existing trust service obligations and ensuring proportional application, particularly for smaller entities.

- **Annex V – Annex VI, Point 2, Use of the term 'data set'**

In point 2, the use of the term 'data set' is confusing. It is not clear whether this refers to the information relating to the identification of the relying party or the datasets it will consume. Generally, the term 'data set'' is used in cases where personal data is processed.

We suggest clarifying this wording or referring to 'information' instead.

- **Annex V – Annex VI, Points 3 and 3(b), Publication of certificate transparency log information**

- **Point 3(a):** the term class in 'WalletRelyingParty class' is not defined in the Annex. It should also be noted that a relying party can have several roles, including that of provider of attribute attestations.

- **Point 3(b)**:

  - The obligation to provide complete wallet-relying party access certificate histories, including certificate transparency log information in accordance with RFC 9162, enhances transparency but may expose historical key configurations and rollover information. Without contextual safeguards, this may create operational security risks and unintended intelligence aggregation opportunities. We therefore **recommend** clarifying the scope and granularity of historical certificate disclosure and assessing whether time-limited or purpose-bound disclosure would achieve the same transparency objective with reduced security exposure.

  - We also have practical questions regarding the interpretation of this requirement:

- The modalities for intermediaries, as reflected in Table 1, are not fully clear. Where intermediaries are involved, the relying party must inform them, but further clarification is needed on the information that is publicly returned via the API.
- For recording data, it is necessary to specify both the Purpose and the associated Personal Data Policy explaining the purpose, in line with GDPR requirements. The interaction with eIDAS Art. 5b(2)(c) is not fully clear and may require adjustments to existing personal data policies.
- The reference to Policy.type as a 'privacy statement' is not immediately clear.
- According to Table 1, it seems that it will also be necessary to indicate the use-cases '*array of IntendedUse objects in order to specify intended use cases in which the wallet-relying party intends to rely on attestations of attributes of a wallet user presented by a wallet unit. IntendedUse is not required from wallet-relying parties that register only to act as a designated intermediary*'. Information about relying parties will be public. However, some information / use cases may not be intended for public disclosure, in particular information relating to agents and certain use cases, whose disclosure could have competitive implications.

- **Annex V – Annex VI, Point 4(b), full registry retrieval without query parameters**

The requirement that the API must return the full list of registered wallet-relying parties where no query parameters are provided may facilitate large-scale data harvesting and create operational strain for national registries. This may also increase cybersecurity exposure and infrastructure costs for Member States.

We therefore **recommend** allowing Member States to implement pagination limits, download thresholds or controlled access mechanisms for full-dataset retrieval while maintaining transparency objectives.

- **Annex V – Annex VI, Data schema requirements (Tables 1-11)**

The Annex introduces extensive mandatory data schemas, including detailed attributes related to identifiers, entitlements, intended use, supervisory authorities and legal bases. While harmonisation is welcome, the multiplicity and mandatory nature of several fields (e.g., support URI, srvDescription, entitlement, supervisory Authority) may create disproportionate operational burdens, particularly for smaller or low risk relying parties.

We therefore **recommend** reassessing whether all listed attributes must be mandatory and considering a proportionate approach based on risk, scope of services and size of the wallet-relying party.

- **Annex V – Annex VI, Intended use schema (Table 2)**

The mandatory listing of purposes, privacy policies and credential specifications within the intended use schema links Art. 5b(2)(c) of Regulation (EU) No 910/2014 with Art. 5(1)(b) of Regulation (EU) 2016/679 (GDPR). Without further clarification, this may create interpretative uncertainty regarding

the relationship between 'intended use' under eIDAS and 'purpose limitation' under GDPR, potentially leading to duplicative documentation requirements.

We therefore **recommend** clarifying the interaction between eIDAS intended-use requirements and GDPR purpose limitation and ensuring that relying parties are not subject to duplicative compliance documentation.

As an additional point, Table 2 does not specify particular constraints on the level of detail to be reported under Art. 5b(2)(c) of the Regulation, apart from the requirement that the purpose be automatically localised into the citizen's language. The format relies on free text, as defined in Table 4, which should allow purposes to be registered using broad categories.

Feedback on the Draft Implementing Act amending Commission Implementing Regulation (EU) 2025/1569 (Articles 45d(5), 45e(2), 45f(6) and 45f(7))

The European Credit Sector Associations (European Association for Co-operative Banks, European Banking Federation, and European Savings and Retail Banking Group – ECSAs) e-ID Task Force would like to share observations regarding the draft implementing regulation prepared by the Commission concerning the updated standards and technical specifications needed to issue qualified electronic attestations of attributes and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source.

- **Art. 1(1)(c) – Art. 4(4), Revocation techniques – privacy preserving and unlinkability**

Art. 4(4), as amended, requires providers to implement revocation techniques that are 'privacy preserving and hindering linkability or traceability' and to comply with Annex II. While this objective is aligned with data protection principles, the provision does not define:

- measurable criteria for 'privacy preserving',
- acceptable levels of unlikability,
- or concrete technical approaches.

This may lead to divergent interpretations and inconsistent implementation across Member States.

We therefore **recommend** defining minimum technical requirements and measurable criteria for privacy-preserving revocation mechanisms in Annex II, including references to recognised standards or implementation profiles.

- **Art. 1(2)(b) – Art. 9(4), Verification result and inclusion of attributes**

- Art. 9(4) allows the verification result to contain the same attributes as those set out in the verification request. This may lead to unnecessary disclosure of personal data and risks of over-processing, particularly where verification could be achieved with a binary or minimal response. This creates potential tension with Art. 5(1)(c) GDPR (data minimisation). We therefore **recommend** clarifying that only strictly necessary data shall be included in the verification result and explicitly limiting attribute disclosure to what is required for the specific verification purpose.

- The amendment to Art. 9(4) uses the wording 'may contain' in relation to the 'verification result', which may create ambiguity as to whether attribute inclusion is intended as an exception, a standard practice or a fully optional choice. Clarification would be helpful to ensure consistent implementation.

- **Art. 1(2)(c) – Art. 9(4a), Verification mechanisms – mandatory compliance with Annex IV**

Art. 9(4a) requires verification mechanisms to follow the specifications set out in Annex IV. Annex IV refers to ETSI TS 119 478 (clauses 6.1.1, 6.2.2 and 6.2.3), which are marked as 'pending adoption'.

ECSA eID TF Secretariat: European Associations of Co-operative Banks, Rue de l'Industrie 26-38, B-1040 Brussels
Tel: +32 2 230 11 24, E-mail: chiara.delloro@eacb.coop
Transparency register: *4172526951-19*

Binding legal requirements to technical specifications that are not yet adopted creates legal uncertainty and implementation risks.

We therefore **recommend** postponing the mandatory application of Annex IV until the referenced standards are formally adopted and introducing transitional provisions or alternative recognised standards.

- **Annex I, Point (1), Normative references to ENISA 'Agreed Cryptographic Mechanisms'**

Annex I refers to the ENISA 'Agreed Cryptographic Mechanisms' without specifying a fixed version. This creates a dynamic reference to an external document that may change over time without formal legislative control. This raises concerns regarding legal certainty and foreseeability.

We therefore recommend introducing explicit versioning of the ENISA document or incorporating the relevant cryptographic requirements directly into the Annex.

- **Annex I, Point (7) – REQ-EAASP-7.5.3-01B, Mandatory compliance with ENISA cryptographic mechanisms**

The requirement to use cryptographic techniques compliant with ENISA "Agreed Cryptographic Mechanisms" further reinforces reliance on a non-binding, evolving external document. Without clear versioning or governance, this may lead to:

- inconsistent implementation,
- compliance uncertainty,
- dependency on external updates outside the legislative process.

We therefore recommend clarifying governance, versioning and update mechanisms for the referenced ENISA specifications.

- **Annex I, Point (8) – REQ-EAASP-7.8-05 and 7.8-06, Frequency of vulnerability scans and penetration testing)**

The requirement for quarterly vulnerability scans and annual penetration tests introduces strict operational obligations. While enhancing security, such fixed frequencies may not reflect risk-based approaches and may impose disproportionate burdens on smaller providers.

We therefore **recommend** allowing risk-based adaptation of testing frequency, considering system criticality, threat level and organisational size.

- **Annex I, Point (4) – REQ-EAASP-6.1-02, Documentation of revocation mechanisms**

The requirement to document revocation mechanisms in the EAAS practice statement enhances transparency but may result in disclosure of sensitive security architecture details. Without safeguards, this may increase exposure to targeted attacks.

We therefore **recommend** clarifying the level of detail required and ensuring that sensitive technical information is protected while maintaining transparency.

- **<u>Annex II – Reference to Implementing Regulation (EU) 2024/2979, standards and revocation techniques</u>**

Annex II introduces a direct dependency on Implementing Regulation (EU) 2024/2979 for both standards and revocation techniques. This creates cross-regulatory dependencies that may:

- increase complexity,
- create risks of inconsistency between legal acts,
- complicate implementation for providers.

We therefore **recommend** ensuring full alignment between both implementing regulations and providing clear guidance on how overlapping requirements should be interpreted and applied.

- **<u>Annex III (Annex IV), Points (a) and (b) – Reference to ETSI TS 119 478, pending adoption</u>**

Annex IV requires compliance with ETSI TS 119 478 specifications that are explicitly marked as 'pending adoption'. This creates a situation where compliance is required with non-finalised technical standards. This undermines legal certainty and may delay implementation.

We therefore **recommend** removing or deferring mandatory references to non-adopted standards and introducing fallback or interim specifications.