



Hackhofergasse 5/16
A-1190 Vienna
phone: +43 676 940 9309

office@european-signature-dialog.eu

ZVR-nr: 579746942

European Commission Consultation on the European Digital Identity Wallets (EUDIW)

ESD recommendations on the Commission draft Implementing Regulations

1. European Digital Identity Wallets - certification
2. European Digital Identity Wallets - protocols and interfaces to be supported
3. European Digital Identity Wallets - integrity and core functionalities
4. European Digital Identity Wallets - trust framework
5. European Digital Identity Wallets - person identification data and electronic attestations of attributes

ESD – our expertise

The European Signature Dialog (ESD) stands as the pinnacle consortium of leading European Qualified Trust Service Providers (QTSPs), facilitating secure digital interactions across Europe every day.

ESD has successfully collaborated with all institutions leading up to the adoption of eIDAS 2. Now, ESD has set up multiple Working groups to address the implementing acts of the eIDAS Regulation that has entered into effect May 20, 2024.

ESD members are European Qualified Trust Service Providers (QTSPs) with extensive expertise in the trust services market. With several decades of experience, ESD members offer a comprehensive range of Trust Services across the digital economies of Europe.

Many of them have previously contributed to the standardization and regulatory efforts to the European Union and to national jurisdictions as well. They continue to do so to this day.



General remarks

ESD welcomes the release of the draft proposal for the Implementing Acts. These are essential for laying the foundation for the implementation of the EUDIW.

However, ESD believes that the points mentioned below can lead to significant improvements, a more consistent implementation, and, as a result, better interoperability and overall acceptance of the Wallet.

- The Implementing Acts submitted for consultation lack sufficient detail and do not adequately reference the technical standards necessary for the homogeneous implementation of wallet solutions.

There is also a risk that the actual homogeneity of the solutions to be defined in each Member State and their actual interoperability will be jeopardized, with the consequent risk that the objectives of the eIDAS2 Regulation will not be achieved.

In particular, it would be appropriate to have explicit references to standards addressing issues such as:

- Trust Model/Trust Establishment between the different roles in the EUDI Wallet ecosystem.
 - PIDs and (Q)EAs issuance.
 - PIDs and (Q)EAs presentation (remote and proximity presentation flows).
 - selective disclosure, zero-knowledge proofs and the ability to unlink.
- ESD favours the implementation of a single EU-wide certification system to ensure consistency and maximize the chances of success for eIDAS. Achieving an EU-wide architecture, only to devolve certification schemes to individual member states, is counterproductive and will undermine the core goals of eIDAS - promoting interoperability, enhancing cross-border trust and security, facilitating digital transactions, and creating a unified digital single market. The impact on wallet providers of having to certify and maintain certification separately in each country will be overwhelming.
 - This is all the more important because national certification schemes may not be harmonized, and there is no mechanism to ensure that the security of these national schemes is equivalent. The European Digital Identity Cooperation Group can only provide recommendations, as outlined in Preamble #10 of the Implementing Act regarding certification, and Article 5c (3) of Regulation 1183/2024.
 - There must also be safeguards to prevent any unfair advantage for state actors who are developing the wallet architecture in parallel with launching and certifying their systems under national certification schemes. These national schemes will be in use until a



European-wide certification framework is established. It is essential to ensure that this does not lead to a competitive imbalance or hinder private sector participation. Clear guidelines should be in place to prevent any potential misuse of this early advantage.

- ESD also believes that treating wallets as "national," with each member state responsible for notification, poses a risk that these states may adopt policies limiting qualified e-signatures or qualified attribute attestations to one or several national QTSPs. Such a move would create a closed ecosystem confined to individual member states, contradicting the legislative intent of eIDAS, which aims to promote mutual recognition and the free use of qualified trust services across the internal market. This approach could raise national barriers, restrict market access for trust services, and distort competition within the EU. To ensure an open digital economy where electronic transactions can flow freely across borders and competition among service providers is encouraged, the choice of multiple QTSPs integrated into any EUDI wallet must ultimately rest with the user.
- The implementation of the EUDIW is a complex and demanding task for all stakeholders in the ecosystem, including regulators, wallet solution providers, QTSPs, and citizens, all of whom require secure, interoperable, and user-friendly wallet solutions. To ensure the timely release and certification of these solutions, the Implementing Acts must reference proven and validated industry standards, technologies, and processes. A key example is the use of qualified certificates issued by QTSPs for wallet relying party access, similar to the successful approach implemented in PSD2 for the financial sector.
- ESD also notes that the proposals for the Implementing Regulations cover several types of certificates, including relying party access certificates, signature or seal certificates, and others, used by relying parties, registrars, registers, and similar entities. However, the draft regulations do not clearly specify how the private keys for these certificates must be protected, and this should be clarified.

In addition to these general remarks on the Commission's proposals, ESD presents the following observations **on each of the five draft Implementing Regulations**:



1. European Digital Identity Wallets – certification

Please consider the following comments regarding the Implementing Regulation on European Digital Identity Wallets – certification¹:

- **Recital (10):** ESD is concerned about the potential lack of harmonization across national certification schemes. Currently, no mechanism exists to guarantee that the security standards of these schemes are equivalent. The European Digital Identity Cooperation Group is limited to offering recommendations (Preamble #10; Art. 5c(3) of Regulation 1183/2024), which may not ensure consistent implementation across member states.
- **Recital (14):** The Implementing Regulation should clearly establish who will define the EU Digital Identity Wallet Trust Mark, how it will appear, and how it can be verified for certified wallets (as referenced in Article 3.4(b) of the Implementing Regulation and Article 3.50 of eIDAS 2.0).
- **Article 2(5)** states that *“National certification schemes shall cover the specific architecture of a wallet solution and of the electronic identification scheme under which that wallet solution is provided. When national certification schemes cover more than one specific architecture, they shall include different sub-schemes, each of which covering a specific architecture.”*

Possible negative consequences:

- Developing the certification scheme in tandem with the wallet solution will require close collaboration between the wallet provider and the member state or scheme owner, which may give state-owned organizations an unfair advantage in developing wallet solutions, effectively excluding private players from the market.
- This approach risks a biased certification process, as designing the wallet architecture, developing the solution, and certifying it would not allow for independent evaluation. To ensure impartiality, the design, development, and certification processes must remain completely separate.

To address this, the Implementing Regulation should explicitly state that the specific architecture of a wallet solution must be aligned with the Architecture Reference Framework (ARF).

- **Article 3.4.d** states that *“responsibilities and the legal action to be taken where certification under the scheme is being used fraudulently shall be established,”* while **Recital (15)** adds: *“In order to discourage fraud, national certification schemes should*

¹ Ref. Ares(2024)5786790 - 12/08/2024



define actions to be taken where certification under the scheme is being claimed fraudulently.”

The schemes should also establish clear requirements for how and where fraudulent activity can be easily reported, including the process for handling such reports and the timeframe for evaluating and responding to them. Although **Article 14** outlines a complaint mechanism related to a certificate of conformity issued, it does not address fraudulently claimed certifications.

- **Article 6.4:** A specific timeframe should be established for the Cooperation Group to provide comments and recommendations.
- **Article 7.3(a)** mentions that *“the essential requirements as set out in Annex I to the Cyber Resilience Act where applicable, or requirements meeting the security objectives set out in Article 51 of Regulation (EU) 2019/881.”*

If one set of requirements is weaker, the certification scheme referencing those requirements could lead to the certification of a less secure wallet solution. The text of the Implementing Regulation should ensure that, in the case of conflicting requirements, the strongest standards are applied.

- **Article 11 and recital (17):** The cancellation of a certificate of conformity can have serious consequences, such as the revocation of all deployed wallet units. Therefore, certification bodies should only consider cancellation if an unremedied vulnerability is likely to significantly impact the reliability of the wallet solution or that of another wallet solution. However, cancellation should not be limited to vulnerabilities alone; it must be possible in all situations where the reliability of the wallet or other wallet solutions is significantly affected.
- **Article 11** states that *“Certification bodies shall suspend without undue delay the certificate of conformity of a wallet solution (...) that impacts its conformity to the national certification schemes’ requirements.”* **Article 16** further states that each Member State must evaluate the consequences of non-compliance and the conditions for the suspension of a certificate of conformity. The suspension “without undue delay” and the subsequent cancellation of certification status have a significant impact and must be weighed against the seriousness of the infringement, according to criteria that are consistent across the Union.

Since **Article 16** allows Member States to define which infringements may lead to suspension, there is a risk of significant variation between the provisions of national schemes. To prevent these disparities, the implementing act should establish uniform criteria and clearly define the seriousness of infringements that can lead to suspension or cancellation.



2. European Digital Identity Wallets - protocols and interfaces to be supported

Please consider the following comments regarding the Implementing Regulation on European Digital Identity Wallets – protocols and interfaces to be supported²:

- **Article 2(13):** To ensure the security and trustworthiness of the wallet relying party access certificate, its issuance must be restricted to a Qualified Trust Service Provider (QTSP) listed on the European Union Trusted List (EUTL).
- **New Article 3.1.1.:** To enable harmonized access across Europe, access certificates should be standardized, with a viable example being the access certificates used in the PSD2 ecosystem. Therefore, we propose introducing a new **Article 3.1.1:** *"With regard to the protocols and interfaces referred to in paragraph 1, wallet providers shall ensure that they support the standard outlined in the Annex."*

Subsequently, the Annex should be updated with: "Standard referred to in Article 3.1.1: ETSI TS 119 495."

- **Article 3:** Please include interfaces for the creation of qualified electronic signatures and seals. This is a core functionality of the EUDIW, and these interfaces are currently missing.
- **Articles 3 and 5.5:** In scenarios involving personal wallets for person-to-person usage, the Wallet-to-Wallet functionality should be removed. In such cases, Wallet-to-Wallet use should only support proximity-based use cases, as broader functionality would pose a high risk of fraud.
- **Article 4.5:** The term "identification n data" should be corrected to "identification data."
- **Article 4.5(a):** Remove the requirement to "request all formats," as issuers typically support only one format. Additionally, issuers publish the format they support.
- **Article 5.1 and Annex:** The standards OpenID for Verifiable Presentation and OpenID for VCI should be included. Referencing only one standard is insufficient, as SD-JWT cannot be implemented with the mdoc protocol.
- **Article 7.3** shall be rewritten as follows: *"Wallet providers shall ensure that wallet units allow wallet users to substantiate the reports, including the authenticated and validated requests from wallet relying parties in addition to the wallet users' claims in machine-readable format."*

² Ref. Ares(2024)5786773 - 12/08/2024



3. European Digital Identity Wallets - integrity and core functionalities

Please consider the following comments regarding the Implementing Regulation on European Digital Identity Wallets – Integrity and core functionalities³:

- **Article 2:** To avoid ambiguity and ensure a harmonized understanding across member states, we suggest adding a definition for the “non-professional use” of the free electronic signature by natural persons. We propose the following definition:
“Non-professional purposes” definition proposal:
Use that refers to activities or actions undertaken by one or more physical persons purely for personal, recreational, or private use, with no connection to any business, commercial, or occupational objectives. These activities are not intended to generate income, profit, or any form of compensation and are not performed on behalf of an organization, employer, or client. Additionally, the documents to be signed are not intended to be provided to a private organization, employer, or legal entity as a Relying Party.
It is essential that member states implement effective and proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to the above-defined purposes. This could include, for example, listing specific cases that qualify as “non-professional,” limiting the number of transactions per case, and ensuring that the costs of providing these services free of charge are borne by the party initiating or benefiting from the transaction.
- **Article 3.2:** Qualified certificates issued by QTSPs must be used. To ensure the security and trustworthiness of the certificates, issuance must be restricted to QTSPs listed on the EUTL.
- **Article 6:** Split “Wallet Unit attestation” into “Wallet Instance Attestation” and “Wallet Trust Evidence,” as outlined in ARF1.4. The current wording should be aligned with ARF1.4 to prevent misunderstandings.
- **Article 12.2:** Please define “signature creation application.” This term is not defined in Article 2 and should be clarified, for example, by referencing **CEN EN 419 241-1**:
“3.12 signature creation application: an application that creates a signed document using the digital signature generated by a SCDev.”
- **Article 12.2(c) vs. Annex III:** The wording in Annex III should be aligned with that of Article 12.2(c) regarding “at least one.” Article 12.2(c) states, “Signature creation

³ Ref. Ares(2024)5786754 - 12/08/2024



applications shall support at least one of the following signature or seal formats," while Annex III requires that "Signature creation applications shall support all of the following signature or seal formats." Given the specificities of certain formats, each wallet provider or signature creation application provider should have the flexibility to choose the most appropriate formats based on their service model.

- **Article 13:** Please specify which data are covered by the data recovery functionality. A precise definition is crucial to avoid any uncertainty.
- **Annex I:** Please add SD-JWT. SD-JWT is an important format and is also covered by ARF 1.4.
- **Annex III, Article 1:** Please define the standard for 1(a). The reference to the standard (ETSI EN 319 142) is missing.
- **Annex III, Article 2:** The wallet should support an interoperable interface between the Wallet and a remote QSCD, allowing the Wallet user to activate a qualified electronic signature or seal. In addition to the CSC API, this interface should be based on common wallet protocols, specifically an extension of OpenID4VP or a new ETSI standard implementing this extension. It should also support the combination of PID and/or credential presentation with the activation of a signature.

We recommend listing the interfaces related to the standards that the wallet must support and mandating their functions, given that no comprehensive standard for QES using the EUDI Wallet exists yet.

- **Annex III:** "Signature and seal formats to be supported by signature creation applications referred to in Article 12" specifies a particular version of the Cloud Signature Consortium APIs (v2.0) to be supported by signature creation applications integrated into Wallet Instances. To allow for future adaptations, especially considering lessons learned from the Large-Scale Pilot projects, it would be appropriate not to specify a particular version of the APIs.



4. European Digital Identity Wallets - trust framework

Please consider the following comments regarding the Implementing Regulation on European Digital Identity Wallets – trust framework⁴:

- **Qualified certificates issued by QTSPs** should be used in **Annex II, Articles 1.10, 2.7, 3.1(g), and 4.1(g)**. To ensure the security and trustworthiness of the certificates, issuance must be restricted to QTSPs listed on the EUTL.
- **Annex II:** eIDAS-compliant means must be used. Every certificate mentioned and every URL should be secured using eIDAS-means.

⁴ Ref. Ares(2024)5786798 - 12/08/2024



5. European Digital Identity Wallets - person identification data and electronic attestations of attributes

Please consider the following comments regarding the Implementing Regulation on European Digital Identity Wallets – person identification data and electronic attestations of attributes⁵:

- **Article 2 (15):** Change definition to *“provider of wallet relying party access certificates’ means a trust service provider (delete: natural or legal person) mandated by a Member State to issue relying party access certificates to wallet relying parties registered in that Member State”*.

To ensure maximum harmonization and interoperability throughout the EU, providers of wallet relying party access certificates should be QTSPs according to eIDAS, otherwise the Member States would have to establish certificates with a specific Level of Assurance, policy and validation process.

- **Article 3** states that *“Member States shall enrol wallet users in accordance with the enrolment requirements set out in Commission Implementing Regulation (EU) 2015/1502.”* While Member States are ultimately responsible for the PID issuance process, it does not seem accurate to assume that they are also responsible for activating wallet users. In fact, the eIDAS Regulation does not explicitly require that the role of the PID provider and Wallet provider be assumed by the Member State. The role of Wallet Provider can, in fact, be delegated to a specific entity or a consortium of recognized entities.
- **Article 5.1:** The policies should be published and made publicly available. The policies outlined in No. 1 are crucial for the functioning of the wallet ecosystem. To ensure the highest level of standardization, additional specifications should be provided regarding the structure and publication location of these policies. This could be modelled on the structure of Trust Service Practice Statements (TSPS).
- **Article 5.4(d):** Change to: *“upon becoming aware that the value of one or more attributes in the person identification data or the electronic attestation of attributes have changed through their own knowledge or through information from authentic sources or other third parties who have confirmed an attribute.”*

⁵ Ref. Ares(2024)5786783 - 12/08/2024



For example, when issuing credentials for chambered professions like medical doctors, the relevant chamber must have the authority to revoke them. The same applies to authentic sources if a license is revoked.

- **Annex:** 'Technical Specifications for Person Identification Data Referred to in Article 3(3)': The Annex currently outlines a set of mandatory and optional attributes for identifying a natural person. However, Article 3(3) of Regulation (EU) 2024/1183 defines "person identification data" as a collection of data issued in accordance with Union or national law that allows for the establishment of the identity of a natural or legal person, or a natural person representing another natural person or a legal person.

While it is implied that "legal representation binding" could be facilitated through electronic attestation of attributes in conjunction with a natural-person PID, there is no explicit mention of identification data for legal entities, which appears to contravene Article 3(3) of the Draft Regulation.

To fully support the use of digital wallets for both personal and professional applications, it is crucial to address this gap. Explicit regulations concerning the identification data of legal entities would mitigate the risk of undermining the interoperability and adoption of these systems.

Therefore, we ask to harmonize the Annex with the Interoperability Framework for the minimum set of attributes for notified electronic identification schemes as established in the Annex of Implementing Regulation 2015/1501.

- **Annex:** Remove "Sex," "Nationality," "Issuing Authority," and "Issuing Country" from the mandatory PID data. The first two are not included in the German eID, and the latter two are redundant, as they are already covered by the "Issuer Certificate."
- **Annex:** The nationality attribute indicates "one or more" country codes represented as tstr, but it does not specify how multiple values should be represented (e.g., using a separator). We recommend making this attribute an array of strings or allowing the attribute to occur more than once.
- **Annex:** The format specifies two different date formats (tdate or fulldate). For simplicity and to ensure clarity, we recommend using fulldate consistently, so there is no ambiguity regarding inclusivity of the data.
- **Annex:** It is not specified that date/time values must include the timezone. We recommend requiring that all times be encoded in UTC for consistency.
- **Annex:** While birth_date and birth_place begin with birth_, family_name_birth and given_name_birth use birth as a suffix. For consistency, we recommend starting all these attributes with birth_.



- **Annex:** Currently, only attributes for age_over_13 and age_over_18 are specified. What about pension age or other commonly used age checks? We suggest allowing more flexibility by introducing age_over_N (where N is the specific age) or an age_over attribute that can occur multiple times and contain the age as a uint.
- **Annex:** The portrait attribute does not specify an encoding format or a minimum resolution for the facial image.