



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)

Recommendations on the Commission draft Implementing Regulations

- 1) European Digital Identity Wallets – security breaches or partial compromise
- 2) European Digital Identity Framework – cross-border identity matching
- 3) European Digital Identity Wallets – registration of relying parties
- 4) European Digital Identity framework – verification of electronic attestation of attributes
- 5) European Digital Identity Wallets – list of certified wallets

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 eIDAS2. 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 second set of draft proposals of Implementing Acts (IAs) as an essential foundation for the implementation of the EUDIW.

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

- **Avoid Reinventing the Wheel**

ESD encourages the Commission to refrain from introducing new or additional technical specifications in the Implementing Acts when existing, proven models are already in place and functioning effectively.

Instead, we recommend leveraging the existing trust services and infrastructure established under the first version of eIDAS.

- **Reference Proven Industry Standards and Leverage Qualified Certificates**

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. These stakeholders require secure, interoperable, and user-friendly wallet solutions. To ensure the timely release and certification of these solutions, the Implementing Acts should reference proven and validated industry standards, technologies, and processes.

In particular, ESD suggests that the Implementing Acts include the use of qualified certificates issued by QTSPs for wallet relying party access and relying party registration.

This approach, modeled after the successful implementation of PSD2 in the financial sector, would provide a robust foundation for trust and interoperability across the ecosystem.



1) European Digital Identity Wallets – security breaches or partial compromise

▪ Annex 1:

The thresholds defined here conflict with the Implementing Regulation of 17 October 2024, which lays down rules for the application of Directive (EU) 2022/2555 regarding the technical and methodological requirements for cybersecurity risk-management measures and the further specification of cases in which an incident is considered significant for [...] trust service providers.

The threshold values in the NIS2 Implementing Regulation, which apply to all trust services (including non-qualified ones), are in some cases considerably stricter - particularly regarding the availability criterion - and result in more frequent reporting events than those defined here for the EUDIW.

Given the higher level of confidence required for the EUDIW, its threshold values should be adjusted accordingly to reflect this sensitivity and therefore be stricter.



2) European Digital Identity Framework – cross-border identity matching

- **Ensure Consistency with Article on Definitions**

ESD proposes ensuring consistency in the structure and logic of the Implementing Acts by including an article on definitions, similar to all other Implementing Acts.

- **Art 2(4):**

The data specified here (name, place of birth, date of birth, and nationality) are insufficient to guarantee a clear match and should be supplemented with additional information.

- **Art 2(7):**

A precise definition of what constitutes an "exact match" should be provided.



3) European Digital Identity Wallets – registration of relying parties

Strengthening Relying Party Identification and Ensuring Resilience in the EUDIW Ecosystem

ESD welcomes the introduction of strong and unambiguous identification of Relying Parties accessing data within the European Digital Identity Wallet (EUDIW). We believe this is a crucial step in building transparency and trust among end users and ensuring the ecosystem's integrity.

To address operational risks, we emphasize that the design of RP Registers should consider High Availability (HA) and Disaster Recovery (DR) architectures, as well as the separation of public (unauthenticated) and private (trusted entities) interfaces. These measures should explicitly account for potential EUDIW-related Distributed Denial of Service (DDoS) scenarios. Rather than prescribing specific architectural principles, we propose focusing on the overarching requirement that **"all registries and services used by the EUDIW or provided for RP"** must be resilient to operational continuity attacks (e.g., DDoS).

This resilience can be achieved through Qualified Trust Services, which adhere to the stringent continuity assurance requirements outlined in eIDAS/NIS2 (e.g., Qualified Validation Services).

Moreover, we believe that the entities ultimately responsible for accessing and using data obtained from the EUDIW should be clearly identified. According to the GDPR, these entities - defined as "Data Controllers" - carry the responsibility for data access and usage. They must be strongly identified and clearly visible to end users whenever personal data from the EUDIW is accessed or utilized.

To ensure these principles are effectively implemented, we recommend the following clarifications to the final text of the Implementing Act:

- Identification of the entity must be conducted using a method with a Level of Assurance "High" (as defined in eIDAS). As a reference, a Qualified Web Authentication Certificate (QWAC), with technical characteristics akin to those used in OpenBanking PSD2 APIs, but with the necessary adaptations, would be suitable.
- The Relying Party to be identified and authenticated must be the actual "Data Controller," as defined under the GDPR. While intermediation by a Data Processor (as per GDPR) may also necessitate prior registration and authentication, if technically feasible within the protocols and APIs, the identity of the "Data Controller" must remain intact throughout the transaction flows and be clearly visible to end users.



- **Art. 2(11) and Art. 2(12):**

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).

The legal definition used here should not rely exclusively on electronic seals and signatures as technical means but should instead adopt a more technology-neutral approach. Otherwise, it may prevent the use of TLS certificates, particularly Qualified Web Authentication Certificates (QWACs), in alignment with the PSD2 model as outlined in Delegated Regulation (EU) 2018/389 (see Art. 7 below).

We recommend emphasizing the use of eIDAS-compliant means, especially “qualified” ones, as eIDAS has established a harmonized governmental framework for qualified trust services, ensuring consistency and reliability across the ecosystem.

- **Art. 2(15) and Art. 2(16):**

To ensure the security and trustworthiness of the wallet relying party registration certificate, its issuance must be limited to Qualified Trust Service Providers (QTSPs) listed on the European Union Trusted List (EUTL).

- **Art. 3(3):**

It should be “qualified,” electronically sealed or signed to enable the validation of the Relying Party Lists through the EU Trusted List.

- **Art. 4(2) lit. a):**

The roles of identification and authorization must be separated. Identification of the relying party and verification of the details should always be conducted by the issuer of the relying party access certificate. A redundant double-check is time-consuming and should be avoided. The registrar should be able to focus solely on the registration process without conducting additional or deeper checks of the relying party. Sufficient protection and trust level assurance are already guaranteed when a Qualified Trust Service Provider verifies all details before issuing the RP access certificate, as the relying party can only access data from the EUDIW using this certificate.

Failure to streamline this process risks non-compliance with time limits and the automation requirements for registration during the initial provisioning of EUDIW, particularly given that electronic attributes and legal entity identities are not yet sufficiently available.



Moreover, provisions should allow for the use of QWACs and QSeals in accordance with the PSD2 model, as established by Delegated Regulation (EU) 2018/389 (see Art. 7 below).

- **Art. 6(3):**

The term "automated" should be removed, as it introduces unnecessary complexity to the registration process. During the start-up phase, electronic attributes will not yet be sufficiently widespread, making manual checks necessary.

- **Art. 6(3)(b):**

This point should be removed, as it is not necessary for the registration process and can be addressed during the application for the RP Access Certificate. Redundant double-checking should be avoided.

- **Art. 7:**

The option to use Qualified Web Authentication Certificates (QWAC) and Qualified Electronic Seals (QSeal) in alignment with the PSD2 model, as outlined in Delegated Act (EU) 2018/389, should be established as one of the permitted methods for Relying Party Access Certificates. This approach would strengthen interoperability across the ecosystem.

Within the PSD2 model, authentication against the wallet interface is performed using QWACs or QSeals (for offline scenarios). The issuing Qualified Trust Service Provider (QTSP) verifies the identity and details of the relying party in accordance with Art. 24 of eIDAS, including the role of the relying party as a verified attribute within the certificate.

The Relying Party accesses the EUDIW interface using QWAC/QSeal as RP Access Certificates. The process involves:

1. Checking whether the relying party's certificates contain the correct attributes for the specific interface and action.
2. Validating the certificate itself by referencing the public EU trust list.

This entire process is automated, takes place within a short timeframe, and ensures secure and efficient access. Once the correct attributes are confirmed and the certificates are validated, access to the EUDIW API is granted, enabling the relying party to perform the necessary actions. At the same time, the relying party is displayed to the user within the wallet as a verified data recipient, ensuring transparency for the wallet user and allowing them to clearly understand to whom their data is being transferred.



The PSD2 model provides an interoperable, harmonized, and European-wide access mechanism, preventing the need for a separate, unique RP Access Certificate for each EUDIW instance. Without such a mechanism, the required trust anchors would need to be specified in a separate policy.

Using eIDAS-compliant mechanisms saves significant time and ensures harmonization across the EU. Additionally, certificate extensions (e.g., roles) should be standardized at the European level, as also outlined in **Annex I**.

- **Art. 9(3):**

More specific requirements for the notification mechanism should be established to ensure the timely revocation of relying party access certificates. A secure and precise reporting mechanism to trigger revocation is a fundamental requirement for effective certificate management.

- **Art. 10:**

A clearly defined storage period should be specified to enhance interoperability. Additionally, there is a contradiction with the recital, which explicitly mentions a 10-year retention period.

The records may be stored using a qualified electronic archiving system.

- **Annex I: 7:**

To ensure the required level of data protection by restricting access to Relying Parties (RP), a basic definition of data groups at the European level is essential.

This definition should be aligned with existing attribute schemes, such as ICAO. If new attributes are introduced that do not align with existing data groups, a new data group should be defined, or the attribute should be associated with a <void/undefined/other> data group.

- **Annex III: 2:**

Non-qualified trust services can be registered in the EU Trusted List or a national Trusted List but are not required to be registered.

Please clarify how this should be managed.



- **Annex IV: Section 2, Sentence 2:**

"The re-issuance of wallet-relying party access certificates for the same signature or seal activation data shall not be permitted" is unclear.

Please provide clarification.

- **Annex IV: Section 3(a):**

In addition to the Trust Anchor, include verification via the EU Trusted List to clarify the possibility of using eIDAS-compliant certificates.

- **Annex IV: Sections 3(c) and 3(e):**

A clear definition of the "freshness" of the required data and information is needed.

How frequently should queries and updates occur? Without clarification, there is a risk of significant divergence in national protection levels.

- **Annex IV: Section 3(j):**

To this end, providers for Certificate Transparency logging must be established within the EU to uphold European sovereignty.



4) **European digital identity framework – verification of electronic attestation of attributes**

Ensuring Functional Separation and Protecting Data Privacy in QEAA Services

The Implementing Regulation should be supplemented with provisions specifying the requirement for functional separation in the provision of QEAA services, as laid out in Art. 45h(3) of eIDAS.

This requirement should clarify that achieving functional separation can be accomplished through separate team structures, a dedicated member at the management level specifically responsible for QEAA, and distinct reporting channels to this individual.

An excessively broad or ambiguous obligation for QEAA providers to store data centrally to meet retention requirements poses significant risks to data protection and user trust in the new trust service. Art. 24(2)(h) of eIDAS requires QTSPs to retain all issued data for the duration relevant to providing evidence in court. However, for QEAA, it should be explicitly stated that this obligation applies only to transaction data and not to the content of electronic attributes.

Failing to make this distinction could effectively result in QTSPs creating a centralized register of verified user attribute data, which would introduce considerable data protection risks as well as vulnerabilities to potential attacks and misuse. Clear limitations must be established to safeguard user trust and ensure compliance with data protection principles.

▪ **Art. 1(6):**

Art. 1. (6) to be updated on a regular basis to keep in line with technology and standards developments and with the work carried out on the basis of Commission Recommendation (EU) 2021/9469, and in particular the Architecture and Reference Framework.

This provision should be more precise regarding the frequency of updates and the process for verifying compliance with standards. It should also specify a grace period and align with the ETSI timeline to ensure clarity and consistency.

General Remark on Definitions:

The definitions provided lack alignment and require harmonization to ensure consistency and clarity between the current Implementing Acts and the legal framework established under the first version of the eIDAS Regulation.



- **Article 2**

(10) 'Wallet secure cryptographic device' means a tamper-resistant device that provides an environment linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations.

The definition of "secure cryptographic device" is not aligned with Implementing Act 1502/2015 and eIDAS Annex II. For instance, Implementing Act 1502/2015 specifies that a secure cryptographic device must "... protect against duplication and tampering as well as against attackers with high attack potential." This discrepancy may result in differing interpretations and should be clarified.

- **Art. 2(12):**

'Critical assets' means assets within or related to a wallet unit that are of such extraordinary importance that their incapacitation or destruction would have a very serious and debilitating effect on the ability to rely on the wallet unit.

How should terms like "extraordinary importance" or "very serious" be defined? It may be more appropriate to use precise terminology such as *integrity*, *availability*, or *confidentiality* to ensure clarity and avoid ambiguity.

- **Art. 3(1):**

Please clarify that QEAs do not require a wallet binding and can also be issued or used independently of a wallet, in accordance with the requirements of eIDAS. While wallet bindings are often discussed at a technical level, such as through a signature using a wallet key, this approach contradicts the wording of the eIDAS Regulation.

- **Art. 4:**

Specific requirements must be established for a mechanism to inform the QEAA QTSP from the authentic source whenever the content of an attribute changes. Without such a mechanism, the QTSP faces a significant liability risk, as it is responsible for ensuring the accuracy of the QEAA content.

A potential consequence of this lack of clarity could be the issuance of only short-term QEAs, which would negatively impact user-friendliness. The defined mechanism should be fully automated and rely on machine-readable elements to ensure efficiency and reliability.



- **Art. 4.1:**

Providers of qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source must have written and publicly accessible policies regarding validity status management. These policies should include, where applicable, the conditions under which such electronic attestations of attributes can be revoked without delay, in accordance with Article 24(4a) of Regulation (EU) No 910/2014.

Additionally, clarity is needed regarding the duration for which information about revocation must be retained. As per Article 24(4a) of eIDAS, this retention must extend "beyond the validity period." This requirement should reference ETSI Standard 119 471 v0.0.10 for further guidance.

- **Art. 6(2)(a):**

It should be "qualified," electronically sealed or signed, to enable validation through the EU Trusted List.

- **Regarding Arts. 7, 8, and 9:**

For instance:

The Commission shall publish the technical specifications used for the catalogue of schemes for the attestation of attributes.

However, no specific deadline is provided for the publication of these technical specifications. When can this be expected?

- **Art. 7:**

In principle, we welcome the mechanism described here, as it facilitates the rapid rollout of QEAA and provides an open, centralized framework for structuring electronic attributes for QTSPs, users, and relying parties.

However, we would like to highlight a potential issue: this open approach may lead to confusing, error-prone, and partially redundant attribute catalogues, which will be challenging to consolidate later. To address this, explicit consolidation mechanisms for merging similar attribute catalogues should be established. Furthermore, a clear commitment and mandate to standardize attribute catalogues at the European level is essential.

Standardized attribute catalogues will enhance the interoperability, security, and functionality of the QEAA ecosystem, ensuring its long-term efficiency and reliability.



- **Art. 7(3):**

Annex VI of eIDAS, as referenced here, is overly vague and therefore insufficient as a starting point. To ensure legal certainty and clarity for member states, QTSPs, and users, these attribute groups require further specification within this implementing regulation. For example, it should clarify which data groups fall under "financial data."

If such specification cannot be achieved within this implementing regulation, it should at least be stated that the minimum attribute list (Annex VI of eIDAS) will be further defined through agreement by the European Digital Identity Cooperation Group.

- **Art. 7(5) and Art. 8(5):**

The term "qualified" should be used, and the document must be electronically sealed or signed to enable validation through the EU Trusted List. Additionally, it should be explicitly stated that applications can be submitted digitally.

- **Art. 8(3):**

It should be explicitly stated that schemes already standardized at the European level, as well as OOTS schemes created under the Single Digital Gateway framework, are proactively included without requiring an application from any party. This approach promotes standardization and consolidation of schemes, preventing the creation of confusing or redundant structures and thereby enhancing interoperability.

- **Art. 8.3(f):**

"One or more namespaces, attribute identifiers, semantic descriptions, selective disclosure descriptions, taxonomy, and data types of each attribute that is part of an electronic attestation of attributes within the scope of the scheme, either by reference to an attribute in the catalogue of attributes in Article 7, or an attribute defined in an analogue way within the scope of the scheme."

What does "an attribute defined in an analogue way" mean? This term is unclear and lacks a definition in eIDAS or any implementing act. Clarification is required.

- **Art. 9(1):**

It should be explicitly stated that only fully automated procedures are permitted as discovery mechanisms. Additionally, the design and requirements for these mechanisms should be made more specific.

Discovery mechanisms are crucial, particularly in decentralized register structures, as they enable QTSPs to identify and interact with the correct authentic source. This



functionality is essential for the proper operation of the QEAA and the EUDIW ecosystem.

▪ **Art. 9(1)(c):**

The option to use QWAC and QSeal in alignment with the PSD2 model, as outlined in Delegated Act (EU) 2018/389, should also be established as one of the allowed methods for verifying attributes against authentic sources or designated intermediaries. This approach would significantly enhance interoperability.

Within the PSD2 model, authentication against the wallet interface is conducted using QWACs or QSeals. It is evident that the responsible bodies of authentic sources - most of which are public registers - will likely need to interact with numerous QTSPs. This complexity is further exacerbated by decentralized register structures in many EU member states, such as Germany, where multiple levels and responsible parties exist.

This situation mirrors the banking sector, where each bank typically maintains its own interface. To implement effectively a model similar to the PSD2 trust model, that is already proven to be working, it would be essential to mandate the publication of interface specifications and the provision of a test environment. This ensures that QTSPs can independently connect to the interfaces without relying on the cooperation of the authentic sources. Such measures would enable the rapid and efficient establishment of a large number of QEAs within the EUDI ecosystem.

Adopting the PSD2 model simplifies attribute access, as the corresponding register already exists in the form of the EU Trusted List. All QEAA QTSPs are publicly and centrally listed there, including, if necessary, the scope of the qualified trust services they provide. This information is then included as an attribute in the QWAC and QSeal certificates, which are automatically validated by the responsible party at the authentic source. This validation determines whether and how the QEAA QTSP should access the respective interface.

For further details, see: Liptak/Wand, *DuD* 2024, 241–245.

▪ **In ETSI TS 119 612 V2.3.1 (v) URI:** <http://uri.etsi.org/TrstSvc/Svctype/EAA/Pub-EAA>

The issuance of non-qualified electronic attestations of attributes as defined in Art. 3(46) of Regulation (EU) No 910/2014 [i.10], issued by or on behalf of a public sector body responsible for an authentic source, acting as a trust service provider and in accordance with that Regulation.

The Implementing Act does not reference ETSI TS 119 612 or the TSL specification. Non-qualified EAAs should also be included in the TSL to prevent potential spoofing of QEAs or the delivery of fraudulent attestations to wallets by non-qualified providers.



- **Proposal to Add a Point (2)(b) to Annex I**

Content of the Addition:

(b) ETSI TS 119 472-1 Vx.x.xx. (yyyy-mm) *Electronic Signatures and Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1: Profiles for Electronic Attestations of Attributes - General Requirements*

Justification:

For attribute attestation services, referencing only point (a) from the "core wallet requirements IR" would compromise the regulation's technology neutrality. The proposed inclusion of ETSI TS 119 472-1 in Annex I is essential, as there are no implicitly referenced standards currently utilized by existing attribute services.

Notice:

According to Article 45d(2): *"The evaluation of compliance with the requirements laid down in Annex V shall be carried out in accordance with the standards, specifications, and procedures referred to in paragraph 5 of this Article."*

While it is acceptable and understandable for the Committee to limit standards for wallets to ensure interoperability, as derived from Article 45d(5), there is no justification to extend this restriction to attribute attestations outside of wallets. The delegation of authority under Article 45d does not grant a mandate to limit non-wallet formats.

For every trust service article, except QWACs and Qualified Attributes, the term "presumed" applies:

*"By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for [trust service]. Compliance with the requirements laid down in Annex [X] **shall be presumed** where a [trust service] complies with those standards, specifications, and procedures."*

This implies that alternatives are possible for all trust services except QWACs and Qualified Attributes, where solutions are limited to the referenced standards.

1. For Qualified Attributes:

- The referenced standards in the Implementing Regulation are identical to those for wallets.
- This prevents the issuance of X.509 Attribute Certificates (X.509AC).
- Referencing ETSI TS 119 472-1 would enable X.509AC issuance.
- X.509AC is widely supported by existing cryptographic libraries and products. Without this addition, ISO 18013 and W3C Verifiable Credentials would require entirely new APIs, imposing unnecessary costs and implementation burdens.



2. For QWACs:

- The referenced standards are the only permissible options.

Adding ETSI TS 119 472-1 ensures flexibility, technological neutrality, and compatibility with existing systems, reducing costs and fostering broader interoperability across the ecosystem.

▪ Annex 1:

In Paragraph 1, please reference ETSI EN 319 401 and ETSI EN 319 403 as general requirements for QEAA QTSPs, unless these are already covered by other referenced standards. This addition will help harmonize requirements and ensure a basic level of security in the provision of QEAA and PubEAA services.

▪ Annex 4(2):

The term "may" should be replaced with "should" or "shall." This paragraph outlines critical measures to ensure the necessary level of protection and prevent misuse scenarios. Making these measures optional risks creating varying levels of protection across member states, leading to fragmentation of the European trust services market. Standardizing these requirements is essential to maintain consistency and trust across the ecosystem.

▪ Annex 4(3):

Mutual authentication between the authentic source and the QTSP using QWAC and QSeal, as outlined in the PSD2 model (see Art. 9(1)(c) above), should be explicitly stated as a valid method for authentic source authentication.



5) European Digital Identity Wallets – list of certified wallets

ESD has no comments on this Implementing Act.

In case you wish more information please write or call us:

European Signature Dialog

EU Transparency Register number: 994150833943-81

Mail to office@european-signature-dialog.eu