

Profiles for Achieving Compliance and Interoperability in the EUDI Wallet Ecosystem

Andreea Prian¹

¹iDAKTO, France

Abstract

The EU Digital Identity (EUDI) Wallet is set to revolutionize the digital identity management in the European Union, offering its citizens the possibility to engage in the digital society in a secure and interoperable way across the Member States. In order to rise to this challenge, it is essential to build and rely on the proper tools when building such an ambitious project.

Keywords

eIDAS, EUDI Wallet, digital identity

1. Current landscape

The development of the EUDI Wallet is built on four key pillars:

1. Regulatory Framework – The concept of the EUDI Wallet originates from the eIDAS Regulation [1], a binding legislative act that applies across the EU. This regulation defines the legal requirements the Wallet must adhere to.
2. Implementing Acts – Several Commission Implementing Regulations (CIR) provide detailed rules for applying the eIDAS legal framework and establish the technical specifications and procedures necessary for compliance.
3. Communication Protocols – To facilitate interactions between third party entities and the EUDI Wallet, the CIR reference various international standards and protocols.
4. Profiles – Profiles define a selected subset of features within a given standard or protocol. By limiting implementation choices, they help to ensure uniform adoption and consistent usage of the Wallet.

Among these four pillars, only the first two are strictly tied to the European Union's regulatory framework. The last two—communication protocols and profiles—extend beyond the EU's jurisdiction.

The protocols and profiles for the EUDI Wallet can be categorized into two categories: credential issuance protocols specifying how credentials are issued and credential presentation protocols, defining how credentials are presented. Currently, the CIR (EU) 2024/2982 [2] references two ISO standards for credential presentation:

- ISO/IEC 18013-5:2021 – For proximity-based presentation.
- ISO/IEC TS 18013-7:2024 – For remote presentation.

Additionally, the Architecture and Reference Framework (ARF) [3] highlights the use of OpenID for Verifiable Credentials and the OpenID4VC High Assurance Interoperability Profile.

These are international specifications designed for a broad range of use cases and legal frameworks, rather than being specifically tailored for the EUDI Wallet. It is therefore crucial to put into balance these standards available on the market with the specific requirements of the EU ecosystem, stemming not only from the eIDAS Regulation, but also from other horizontal frameworks, like the GDPR and the EU governance rules.

While examining if the legal requirements are covered in their entirety by the specifications referenced, multiple gaps have been identified and the next section of this paper will explore some of them.

TDI 2025: 3rd International Workshop on Trends in Digital Identity, February 3, 2025, Bologna, Italy

✉ andreea.prian@idakto.com (A. Prian)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

2. Examples of identified gaps

2.1. A user-centric wallet

The EUDI Wallet aims to empower users by putting them in control over their personal data. The eIDAS Regulation introduces the concept of sole control of the users, while the ARF repeatedly emphasizes the importance of user consent. Despite being a fundamental aspect of Wallet interactions with other entities, existing protocols do not address these concepts.

To ensure proper implementation, Wallet developers require clear guidance on handling user interactions, particularly consent management. The information presented to users must be both comprehensive and easily understandable. A critical aspect of this is transparently displaying the scope of consent, as the Wallet's presentation protocol will be used across various operations with distinct legal implications. A few examples of such operations are presenting data in order to get access to an online service, electronic signing, and performing payments.

Given these varied use cases, it is essential that users fully understand what they are consenting to whenever they approve a transaction. Establishing clear, standardized guidelines for consent collection and user interaction design will be crucial to ensuring compliance, usability, and trust in the EUDI Wallet.

2.2. Data processing

As part of ensuring GDPR compliance, the handling of the “intent_to_retain” field—specified and mandated in various technical specifications—requires further clarification. This field is a binary flag (true/false) set by the Relying Party in its request to the Wallet for each required attribute. When set to true, it indicates that the Relying Party intends to store the attribute beyond the duration necessary to complete the real-time transaction.

Additionally, as part of its registration process, the Relying Party must comply with GDPR requirements, which include defining a data processing policy that specifies the purpose of data collection and the applicable retention period. However, a key challenge arises in how the Wallet should manage the “intent_to_retain” field in relation to this policy—particularly if discrepancies occur between the declared intent and the established data retention rules.

Clarifying how Wallet implementations should handle these potential conflicts is essential to ensuring both regulatory compliance and user transparency.

2.3. Relying Party Authentication

The regulation also requires the EUDI Wallet to ensure that Relying Parties can be authenticated. To meet this requirement, the implemented protocols must mandate Relying Party authentication and incorporate mechanisms that enable its verification—such as enforcing the use of signed requests.

Additionally, all signed artifacts must be validated against a well-defined set of rules. Specifications are needed to establish what constitutes a valid signature, as multiple verification steps may be required beyond basic cryptographic checks. These may include attribute-specific validations to ensure compliance with security and legal requirements.

Certificate validation is another critical aspect. Currently, there is no standardized validation algorithm defining the constraints that should be applied to certificates—particularly regarding which trusted list should be used to identify the corresponding trust anchor.

Further guidance is essential to clearly define what qualifies as a valid signature, ensuring that only legitimate requests from authenticated Relying Parties are accepted.

2.4. Wallet-to-wallet interactions

A specific case of credential presentation can occur in the form of Wallet-to-Wallet interactions, where one Wallet acts as a Relying Party, requesting information from another Wallet. However, this scenario

raises several important questions:

- How does the sender Wallet authenticate itself?
- What constraints should apply to the request?
- Is a signed request mandatory, and if so, which key should be used for signing?
- What validation rules must the recipient Wallet enforce? (e.g., authenticating the sender Wallet or validating a Wallet unit attestation)
- How should the right-to-ask be verified? This is particularly critical when the requesting Wallet represents a legal person Wallet.

Given the unique characteristics of Wallet-to-Wallet interactions, clear specifications and guidelines are needed to ensure secure, standardized, and legally compliant exchanges.

2.5. Trust ecosystem

Trusted lists play a critical role in establishing certainty within the EUDI Wallet ecosystem, as they provide the status of specific services at a given point in time. Serving as a pillar of the trust framework, these lists enable key functionalities such as identification, authentication, and signature validation.

Existing eIDAS-related trusted lists already cover trust services currently deployed in the Member States, and additional lists are expected for new entities interacting within the Wallet ecosystem—such as Wallet Providers, PID Providers, and Access Certificate Authorities. These lists might contain various details, including: identifiers and service types, service start and end dates, associated certificates which will serve as trust anchors, etc. Whenever an authentication or certificate validation takes place, information from the trusted list must be retrieved and analyzed according to yet to be defined validation procedures.

Additionally, one of the most sensitive aspects in instantiating an EUDI Wallet is establishing trust in the Wallet Secure Cryptographic Device (WSCD)—the component responsible for performing secure cryptographic operations. However, no technical or operational guidance currently exists to address establishing trust in such devices that can originate from various manufacturers. It remains unclear whether a trusted list will also be required for this purpose.

2.6. Algorithms

Finally, the governance framework for cryptographic mechanisms within the EUDI Wallet ecosystem should also be addressed. The EU should establish an official list of approved algorithms that are to be implemented for the EUDI Wallet. This list should take into account the ecosystem specificities, technical limitations that might exist due to the various WSCD types and be practical in order to tackle cumbersome algorithm negotiation between the Wallet and relying parties.

3. Conclusion

The few gaps identified in this paper stem from regulatory requirements specific to the European Union. These gaps exist because the referenced standards, protocols, and specifications are designed for international and multi-purpose use cases, rather than tailored to the EUDI Wallet's unique context.

Developing EUDI Wallet-specific profiles based on existing specifications would enable a more precise response to the regulatory requirements and would support a globally aligned approach, fostering coherence across the various standards and protocols developed by different working groups and organizations.

Beyond ensuring legal compliance, European profiles would play a critical role in achieving effective interoperability and mutual recognition across the European Union.

References

- [1] European Parliament and Council of the European Union, Regulation (EU) 2024/1183, in: Official Journal of the European Union, 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>.
- [2] European Parliament and Council of the European Union, Regulation (EU) 2024/2982, in: Official Journal of the European Union, 2024. URL: https://eur-lex.europa.eu/eli/reg_impl/2024/2982/oj.
- [3] European Commission, Architecture and Reference Framework, 2025. URL: <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.7.1/architecture-and-reference-framework-main/>.