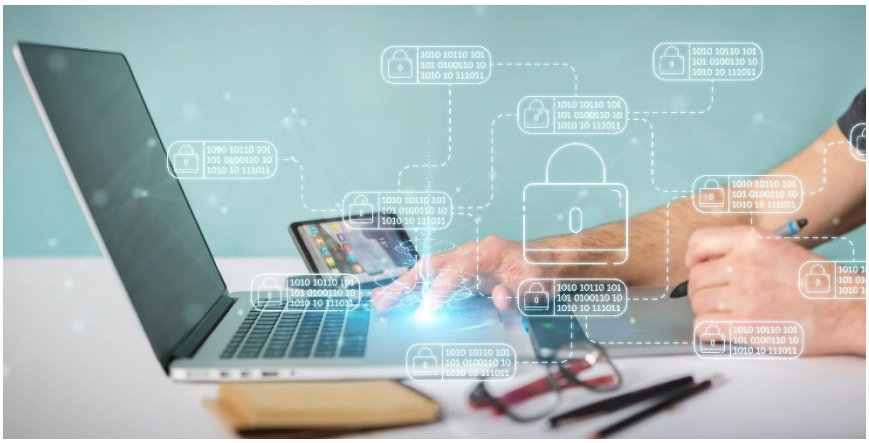
A-SIT

Secure Information Technology Center – Austria

Wallet
Embedded Disclosure Policies



Wallet Embedded Disclosure Policies

Author:
Stefan More
Mail: stefan.more@a-sit.at
April 2025

Abstract:

Article 5a (Paragraph 5e) of the current eIDAS Regulation ("eIDAS 2", 2024) introduces so-called Embedded Disclosure Policies. These allow an issuer (Provider) of electronic attribute attestations to define which service providers are permitted to access the issued document.

An example would be an electronic credential containing personal attributes that should only be accessible to government authorities. This policy is encoded in a machine-readable format and embedded in or attached to the credential (the attribute attestation) and is enforced by the wallet software.

As part of this report, we analyze the current state of the eIDAS 2 regulatory framework and technical framework (ARF) regarding embedded disclosure policies. In addition, we explore further possibilities beyond the applicable implementing acts and the current technical framework.

Contents

1. Introduction

The digital landscape in the European Union is undergoing a significant transformation with the establishment of the European Digital Identity (EUDI) Framework, primarily driven by Regulation (EU) No 910/2014, known as "eIDAS" [1], and its 2024 amendment ("eIDAS 2") [2]. This regulation aims to ensure the proper functioning of the internal market and provide an adequate level of security for electronic identification means and trust services across the Union. Its goal is to enable and facilitate the safe participation of natural and legal persons in digital society and their access to online public and private

services throughout the EU. A cornerstone of this framework is the European Digital Identity Wallet (EUDI Wallet). The EUDI Wallet is an electronic identification means that empowers users to securely store, manage, and validate their person identification data (PID) and electronic attestations of attributes (EAA). Users can then present this data to relying parties and other Wallet users. Each EU Member State is mandated to provide at least one EUDI Wallet by December 2026.

The EUDI Wallets represent a crucial advancement towards a secure and interoperable digital identity ecosystem across the Union, prioritizing the protection of personal data and privacy while facilitating seamless access to services. EUDI Wallets are designed to be user-centric, giving individuals full control over their attributes and privacy. Users have transparent information about what attributes are being presented and to whom, with measures taken to prevent tracking by Relying Parties, PID Providers, or Attestation Providers.

A key feature introduced to enhance privacy and control are embedded disclosure policies (EDPs). They are defined as "*a set of rules, embedded in an electronic attestation of attributes by its provider, that indicates the conditions that a wallet-relying party has to meet to access the electronic attestation of attributes*". In plain language, Embedded Disclosure Policies allow Providers of attestations to specify what relying party can request the attestation. Wallets are then required to process these common embedded disclosure policies and inform the user of the result, allowing the user to make an informed decision to approve or deny the presentation of requested attributes. In doing so, they are a crucial component of the EUDI framework, enabling more sensitive use cases and increasing user trust in the system.

2. Background

2.1. Legislation and Specification Process

The EUDI framework and the Embedded Disclosure Policy mechanism are introduced and defined by several legal texts and technical specifications:

1. The EUDI framework is introduced by the amended eIDAS regulation proposed by the European Commission and adopted by the European Parliament together with the EU Council as representative of the EU member states [2].
2. The implementation of the EUDI framework is supported by a structured process involving Commission Implementing Regulations (CIRs), also known as Implementing Acts (IAs), which clarify the technical details left open by the eIDAS Regulation [3].
3. The Architecture and Reference Framework (ARF) further develops the concepts and specifications based on these legal texts, serving as a reference for uniform implementation and defining technical specifications, standards, and procedures [4].
4. CIRs and the ARF together also rely on existing and established technical standards and specifications. This increases adoptability and reliance of the framework.

2.2. eIDAS EUDI Architecture & Trust Model

The EUDI Wallet ecosystem involves several key roles:

- Users, who control their Wallet Units to receive, store, manage and present attestations
- Person Identification Data (PID) Providers and Attestation Providers, who issue digital attestations to Users. As part of these attestations the providers create and embed disclosure policies.
- Relying Parties (RP), who request and these attributes from wallets and process the resulting presentation of attributes. A RP is a public or private service that relies on the wallet for authentication or attribute verification. RPs must register in the European or national registry, obtain a wallet-relying-party access certificate (an eIDAS2 concept), and optionally a registration certificate detailing which attributes they intend to request. These certificates (signed by designated national Certificate Authorities) establish the RP's identity and declared purpose. During the processing of a presentation request, a wallet checks the corresponding attestations and decides if the wallet is authorized to request the attestation.

The interactions primarily occur in two main flows: issuance of attributes to the Wallet, and presentation of attributes by the Wallet to a Relying Party. To establish trust in an attestation's Provider (issuer), the wallet checks the eIDAS trust(ed) status list.

These relationships are also visualized in Figure 1. This diagram shows core entities and flows. The Wallet Unit on the user's device interacts with Relying Party services on the right and with Identity (PID) / Attribute (Attestation) Providers on the left. PID and Attestation Providers appear in national Trust Lists of certified issuers. Relying Party CAs appear on a national RP Trusted List and use Access and Registration Certificates to authenticate to the wallet [6, 7]. The figure also highlights standard interfaces: e.g. OIDC4VP for presentation and standard credential formats (W3C VC) [8, 9]. In practice, a wallet verifies signatures by checking trust lists: for example, to authenticate an RP, it checks that the RP's access certificate chains to a trusted root listed in the RP Access CA trust list.

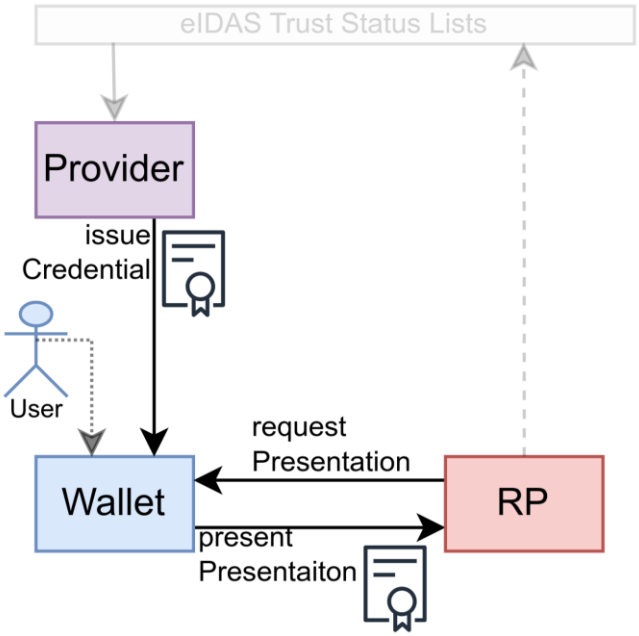


Figure 1: (Simplified) EUDI architecture focusing on Attestation Issuance & Verification

3. (Embedded) Disclosure Policies

3.1. Definition

Embedded Disclosure Policies (EDPs) are machine-readable rules embedded into an Electronic Attestation of Attributes (EAA) by the attribute Provider. These rules define under what conditions, and by which relying parties (RPs), the attestation may be accessed and processed. The EUDI Wallet is required to evaluate these policies upon each presentation request, ensuring that the RP is authorized according to the embedded policy before revealing any user data. In other words, when an Attestation Provider issues an EAA (credential of user attributes), it can include a policy object saying "only these RPs (or RPs with these certificates) may receive this credential". The intent is to prevent user attributes from being disclosed to unauthorized or inappropriate parties. This mechanism enhances user privacy and gives issuers control over how their credentials may be used downstream.

3.1.1. Regulatory Framework

The basis for Embedded Disclosure Policies is introduced in Article 5a of the eIDAS regulation [2], defining that EUDI Wallets shall

in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the permission to access such attestation; [2, Article 5a (5) (e)]

The corresponding Implementing Acts [3] further specify that

embedded disclosure policies should warn the wallet users against inappropriate or illegal disclosure of attributes from electronic attestations of attributes.

Wallet instances shall verify whether the wallet-relying party complies with the requirements of the embedded disclosure policy and inform the wallet user of the result [3, Article 10].

Annex III of Commission Implementing Regulation (EU) 2024/2979 [3, Annex III] outlines the following common embedded disclosure policies that must be supported (as of April 2025):

- 'No policy': Indicates that no policy applies to the electronic attestations of attributes and any relying party can request it.
- 'Authorized relying parties only policy': Specifies that wallet users may only disclose electronic attestations of attributes to authenticated relying parties explicitly listed in the disclosure policies.
- 'Specific root of trust': This option acts as a more flexible alternative. It indicates that wallet users should only disclose the specific electronic attestation of attributes to authenticated wallet-relying parties whose access certificates are derived from a specific root or list of specific roots or intermediate certificates. This allows the provider to restrict the attestation's usage to, for example, a specific sector (e.g., health, education) or enterprise (e.g., a specific company).

In all cases, the wallet is *not allowed* to override a policy to send data to a disallowed party without explicit user consent. If no policy is embedded, the default is unconstrained sharing (subject only to user consent). These templates are intentionally simple: each policy is either an allow-list of RPs or an allow-list of roots. The ARF clarifies that wallets must implement support for the "authorized RPs" and "root of trust" policies, processing the lists in combination with the RP's data.

3.1.2. Technical Framework

In the EUDI Architecture and Reference Framework (ARF), Embedded Disclosure Policies are addressed as part of the credential lifecycle and Wallet-RP interaction model. From a technical perspective, EDP enforcement consists of several steps:

1. Policy Embedding: During the issuance phase, the Provider includes the relevant Disclosure Policy inside the attestation as a structured and signed element, using a standardized format.
2. RP Authentication & Certificate Evaluation: When a presentation request is made, the Wallet authenticates the RP and extracts its metadata, including its certificate chain or access token. The wallet must also verify that the RP's access certificate chains to a trusted root (via trust lists)
3. Policy Evaluation Engine: The Wallet's Disclosure Policy engine evaluates the RP identity against the embedded rules. For example, it checks if the RP's certificate matches an entry on an allowlist or if it chains up to a permitted root.
    a. For an "authorized RPs only" policy, check if the RP's identifier appears in the list.
    b. For a "root of trust" policy, check if the RP's certificate chain contains one of the allowed roots.
4. User Notification and Consent: If the RP is authorized, the Wallet presents the disclosure request to the user, including policy-based information (e.g., "This attestation may only be shared with authorized health sector providers"). The user can then approve or deny the request.
5. Presentation and Logging: Upon approval, the attribute is disclosed as part of a presentation, and the action is logged for accountability, in line with eIDAS transparency and auditability requirements.

In practice, these checks are automated in the wallet software. Article 10 of CIR 2024/2979 mandates that "wallet instances shall verify whether the wallet-relying party complies with the requirements of the [EDP] and inform the wallet user of the result" [3]. The ARF elaborates that if a policy check fails, the wallet should either abort the transaction or present a warning to the user. Thus, EDP enforcement is a runtime step embedded in the wallet's presentation workflow.

EDPs are intentionally issuer-centric: the Attestation Provider (e.g. a company or government) decides the policy, and the wallet enforces it. This differs from typical self-sovereign identity models, where only the user's consent and attribute selection govern disclosure. Here, the issuer adds an extra layer of control.

4. Discussions & Outlook

Although not a technical limitation, embedding a policy may impact user experience. Wallets must present clear messages if a policy blocks disclosure. Recital 8 of the Regulation explicitly calls for "appropriate warnings" [2]. Designing intuitive prompts (e.g. "Your driving license cannot be shared because this app is not on the approved list") will be important for user trust. If policies are too strict or too opaque, users or relying parties might find workarounds or be confused.

4.1. Limitations

While the current regulatory and technical frameworks define basic disclosure policy capabilities, several challenges remain:

- Expressiveness: Current common policies cover basic access control scenarios but may not support complex policy logic, such as temporal constraints or contextual conditions (e.g., "only if the user is in a specific location") [5].
- Interoperability: Variations in credential formats and cryptographic infrastructures across sectors or member states may hinder uniform policy enforcement.
- Revocation & Policy Updates: Once an attestation is issued with an embedded policy, updating or revoking that policy without reissuing the credential is technically challenging and not yet fully addressed in the ARF.
- Trust Bootstrapping: The management of "specific roots" requires robust trust anchor governance mechanisms. It remains unclear how these roots will be registered, distributed, and maintained across different Member States and sectors.

4.2. German "Architekturkonzept" and Policy Enforcement

The German Federal Ministry of the Interior (BMI) has published a national architectural concept ("Architekturkonzept") for EUDI Wallet implementation, which elaborates on how embedded disclosure policies (EDPs) may be managed and enforced in practice.

A critical discussion in the German context concerns whether embedded disclosure policies should be interpreted as hard constraints (enforced regardless of context) or advisory flags (that inform but do not mandate enforcement). The German approach leans toward a strict enforcement model, wherein policies embedded by the issuer are binding, and wallets must refuse to disclose credentials to unauthorized parties without exception. This strictness is intended to ensure legal compliance and user protection but raises questions about policy flexibility and update mechanisms.

Further, Germany's implementation highlights gaps in revocation and update procedures for EDPs. Once a credential is issued, the static nature of EDPs means any change in access permissions requires a complete reissuance. German stakeholders have proposed that future iterations of the ARF include hooks for policy revocation endpoints or dynamic evaluation APIs that could introduce greater adaptability, without compromising the issuer's intent.

5. Other Authentication & Authorization mechanisms

Embedded Disclosure Policies provide a flexible mechanism for Attestation Providers to control access to the data they issue. To do so, they rely on authentication information provided by the Relying Party (RP). In eIDAS, this authentication information is issued to Relying Parties in the form of certificates [2, 6]. These certificates are issued by registration entities that control access to the eIDAS ecosystem. They only issue certificates after verification of the RP's legal identity and registration of the RP's services.

eIDAS 2 specifies two types of Relying Party Certificates [6, 7]:

- Relying Party Access Certificate: Used for granting access to the eIDAS ecosystem to an RP, and authenticating that RP at wallets. Contains basic identity information about the RP that is displayed to the wallet user and can be used by an embedded disclosure policy.
- Relying Party Registration Certificate: The second authorization mechanism in addition to embedded disclosure policies. Defines a set of attributes or attestations that a RP is allowed to request in machine readable form. Using this information, a wallet can check if the RP has registered a use case/service that justifies the attestation request. For example, a service that only requires verification if the user's age is above 18 does not grant the RP permission to ask for other data (or even the user's date of birth). In the current IA cycle the issuing of registration certificates is optional which raises privacy questions. Further, it increases the overall system complexity since wallets now need to deal with an absent registration certificate.

6. Related Work

6.1. EBSI Policies

The European Blockchain Services Infrastructure (EBSI) includes a policy framework for Verifiable Credentials that resembles EDPs in key respects. In EBSI:

- Presentation Policies (PresentationPolicy) are attached by the issuer to a Verifiable Credential as part of the termsOfUse property. This mirrors EDPs, as it allows the issuer to define rules governing who may access or verify the credential.
- Verifier Authorisation (VerifierAuthorisation) is a declaration provided by the verifier/relying party to the wallet during the presentation request. It indicates what attributes the verifier is allowed to request, analogous to the eIDAS 2.0 Relying Party Registration Certificate.

The two-policy model used in EBSI aligns conceptually with eIDAS 2.0's issuer-controlled and RP-declared authorization mechanisms. However, EBSI operates within a decentralized, blockchain-supported identity ecosystem, whereas eIDAS 2.0 follows a top-down, trust-list-based model. Nonetheless, the design patterns suggest future harmonization opportunities between the frameworks.

6.2. ISO/IEC 18013-5 ("ISO mDL/mDOC")

The ISO/IEC 18013-5 standard, particularly its second edition in development by ISO WG10, includes related features. A key concept under discussion (Task AP97.06) involves enabling relying parties to declare their intended data use. This is embodied in the concept of PurposeHints, which let the RP signal the purpose for which data is requested (e.g., age verification, address confirmation).

While not an access control mechanism per se, PurposeHints are designed to enable more privacy-aware interactions and allow credential holders (users) or their software (wallets) to make informed decisions about disclosure. This resembles the user-informed consent model in eIDAS 2.0 and could serve as a complementary or alternative strategy to issuer-imposed EDPs. The ISO approach is especially relevant as ISO mDOC and eIDAS 2.0 increasingly converge through cross-standard credential compatibility (e.g., ISO mDL as a format for EAA).

6.3. German "Berechtigungszertifikate"

Some national systems (e.g., Germany's current eID) use RP certificates ("Berechtigungszertifikate") and registries, conceptually similar to the Access and Registration Certificates in eIDAS 2. The EUDI model can be seen as a pan-European generalization of these trust-based schemes. Unlike corporate single sign-on (SSO) or OAuth systems, the EUDI Wallet emphasizes legal trust frameworks and user consent rather than centralized authorization servers.

7. Conclusions

Embedded Disclosure Policies (EDPs) introduce a novel, issuer-defined layer of privacy control in the EU digital identity framework. Legally mandated by eIDAS 2 and its implementing acts, EDPs require European wallets to honor issuer-specified restrictions on attribute sharing. In practice, wallet software must verify each incoming attestation's EDP against the authenticated relying party, warning the user if the party is not authorized. This complements the wallet's built-in selective disclosure and pseudonym features to enhance data minimization.

However, the current EDP mechanism is limited in scope. Only three basic policy types are supported (no policy, allow-list of RPs, allow-list of CA roots). It lacks fine-grained or dynamic conditions. The reliance on trust lists and certificates adds complexity in cross-border scenarios, and revocation of policies is not directly addressed. Research suggests that future enhancements could leverage the RP registration certificates for more nuanced authorization.

In summary, EDPs are an important step towards privacy-aware credential sharing under eIDAS 2. They reflect a balance between user control and issuer trust: users are informed and only disclose to trusted parties, while issuers retain confidence that their data is not misused. As implementations roll out, close attention must be paid to usability (clear warnings), standardization (trust lists, identifiers), and potential extensions (richer policies, revocation support). The EUDI Wallet architecture (combining European trust frameworks with modern VC standards) provides a solid foundation. The evolution and effectiveness of EDPs will depend on ongoing policy refinement and technological innovation.

References

[*] OpenAI. ChatGPT (o3) [Large language model] was used to edit the text.
[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
[3] Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets.
[4] European Digital Identity: Architecture and Reference Framework (https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework).
[5] More, S., Heher, J., Fasllija, E., & Mathie, M. (2024). Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems. In ARES 2024 - 19th International Conference on Availability, Reliability and Security, International Workshop on Emerging Digital Identities. Association for Computing Machinery (ACM).
[6] Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties.
[7] Fasllija, E., & More, S. Guardians of the Registry: Certificate Transparency for Relying Party Authorization in eIDAS 2. In ARES 2025 - 20th International Conference on Availability, Reliability and Security, International Workshop on Emerging Digital Identities. Springer.
[8] OpenID for Verifiable Presentations - draft 29 (https://openid.net/specs/openid-4-verifiable-presentations-1_0.html).
[9] Verifiable Credentials Data Model v2.0 (https://www.w3.org/TR/vc-data-model-2.0/).