EWC Legal Person Wallet Definition Document v1.0

EWC

EWC LEGAL PERSON WALLET DEFINITION DOCUMENT

Executive Summary

The objective of an EUDIW for legal persons is to enable legal persons to issue and store attestations, create and share presentations in a secure and interoperable manner across public and private sectors, while ensuring compliance with European regulations.

This document serves as a summary of the work done in EWC to explore the role of the EUDIW for legal persons and the functions needed. It also defines a concept of a digital wallet for legal entities under the European Digital Identity Wallet (EUDI) initiative. The beginning of this document sets the legal context with eIDAS2 and provides key definitions, architecture, and functional requirements for the design and operation of legal person wallets.

This document outlines the roles of Issuers, Holders, and Relying party/Verifier (RP)V, as well as the architecture necessary to support the use cases for legal persons. It also describes some usage patterns and interactions specific to legal persons, helping wallet providers understand the key differences between legal person and natural person wallets.

1. Introduction and background

1.1. Scope and objective of the document

The object of this document is to give some insight into the following topics:

1) What is a Legal Person Wallet?
2) Importance of Legal Person Identity Wallet;
3) Key Benefits and Features.

1.2. Context

The work in EWC is based on the following frameworks and assumptions:

- eIDAS2;
- ARF version 1.2;
- ARF version 1.4 for definition of wallet provider attestations: Wallet Instance Attestation (WIA) and Wallet Trust Evidence (WTE). The WIA will be shared will all actors and attests to the trust in the wallet instance, while the WTE is only shared with issuers as it attests to the safe storage of keys and include details on key materials;
- Every actor utilises an EUDIW regardless of role, including relying parties;
- Trust is based on mutual exchange of PID and WIA;
- A conceptual model of a wallet solution, as shown in chapter 3.2;
- Every issuer is responsible for revocation.

1.3. Terminology

This document uses the terminology introduced by the European Commission Architecture Reference Framework (ARF), v1.2.0.

In addition, the following terms are used and specified here:

Term	**Meaning TDB**
Attestation	General term used for Qualified and non-qualified Electronic Attestation of Attributes ((Q)EAA) and natural / legal Person Identification Data (N/LPID) when there is no need to distinguish between different types of electronic attestations of attributes.
End user	A natural person who is interacting with a wallet application. An end user is the final individual or operator who directly interacts with a product, system, or service through its graphical user interface (GUI) to accomplish specific tasks or goals.
EUDIW	European Digital Identity Wallet
HLR	High-Level Requirements
Holder	An entity that receives, controls, manages and presents attestations. (Lodderstedt, Yasuda, & Looker, 2023)
Issuer	An entity that issues attestations (Lodderstedt, Yasuda, & Looker, 2023)

LPID	Legal Person Identification Data
SME	Small and Medium Enterprises
PID	Person Identification Data
	Note: it is used synonymously to express a QEAA/PubEEA for PID
PID Provider	A Member State or legal entity providing Person Identification Data to Users.
Presentation	General term used for (Qualified) electronic presentation of attributes ((Q)EPA) when there is no need to distinguish between different types of electronic presentation of attributes.
(Qualified) electronic presentation of attributes (Q)EPA	(Q)EPA is sent in response of a request for attributes or attestations from a relying party.
Relying party	An entity that requests, receives, and validates Verifiable Presentations. (Lodderstedt, Yasuda, & Looker, 2023)
Revocation Registry	A Verifiable Data Registry for revocation information. See the definition of Verifiable Data Registry (VDR) for more information.
User	A natural or legal person controlling a EUDIW
Verifiable Data Registry (VDR)	A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as attestation schemas, revocation registries, issuer public keys, identifier namespaces etc., required to use attestations.
Wallet application	An optional user interface with functionality to support LoA High that interacts with the wallet core component (WCC)
Wallet instance attestation (WIA)	The Wallet Provider issues a Wallet Instance Attestation (WIA) to the Wallet Instance. The WIA contains information allowing a PID Provider, an Attestation Provider, or a Relying Party, to verify that the Wallet Provider did not revoke the Wallet Instance Attestation (and hence the Wallet Instance itself). When requesting attributes from a Wallet Instance, a Relying Party Instance: • verifies that the Wallet Instance is in possession of the private key belonging to the public key in the WIA. This proves that the Wallet Instance is authentic and is provided by the trusted Wallet Provider. From ARF v1.4
Wallet Core Component (WCC)	The Core component of the wallet solution with the functionality to support communication between wallet instances for instance.
Wallet Provider (WP)	An entity responsible for the operation of an eIDAS-compliant EUDI wallet solution that can be instantiated
Wallet solution	The entire product and service owned by an EUDI wallet

Co-funded by the European Union

	provider, offered to all users of that solution. Source: ARF
Wallet Trust Evidence (WTE)	The EUDI Wallet Provider issues a Wallet Trust Evidence (WTE) to the Wallet Instance. The WTE has two main purposes: • It describes the capabilities and properties of the Wallet Instance, the User device and the WSCD(s). This allows a PID Provider or an Attestation Provider to verify that the Wallet Instance complies with the Provider's requirements and therefore is fit to receive a PID or an attestation from the Provider. • Moreover, the WTE contains a WTE public key. During the issuance of a PID or an attestation (see section 6.6.2.3), a PID Provider or Attestation Provider can use this public key to verify that the Wallet Instance is in possession of the corresponding private key. From ARF v1.4

1.4. Keywords

This document uses the capitalized key words 'SHALL', 'SHOULD' and 'MAY' as specified in RFC 2119, i.e., to indicate requirements, recommendations and options specified in this document.

In addition, 'must' (non-capitalized) is used to indicate an external constraint, i.e., a requirement that is not mandated by this document, but, for instance, by an external document such as [ARF]. The word 'can' indicate a capability, whereas other words, such as 'will', and 'is' or 'are', are intended as statements of fact.

2. Legal text

The following texts are excerpts from eIDAS2 Regulation.

2.1. Recital

Recital 34 and article 48a (2a) show that member states shall provide EUDI wallets to legal persons.

Recital:

(16) *Member States should rely on the possibilities offered by this Regulation to provide, under their responsibility, European Digital Identity Wallets for use by the natural and legal persons residing on their territory. To offer Member States flexibility and leverage the state-of-the-art technology, this Regulation should enable provision of European Digital Identity Wallets directly by a Member State, under a mandate from a Member State, or independently of a Member State, but recognised by that Member State.*

2.2. Article 5a

Article 5a states that all members will provide EUDI wallets for legal persons.

Article 5a – European Digital Identity Wallets:

(1) For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet within 24 months of the date of entry into force of the implementing acts referred to in paragraph 23 of this Article and in Article 5c(6).

2.3. Article 5a.5a

Article 5a.5a states that there must be available functionalities for relying parties to requesting, validating, and sharing person identification data and electronic attestations.

Article 5a.5a - European Digital Identity Wallets shall, in particular support common protocols and interfaces:

> *(ii) for relying parties to request and validate person identification data and electronic attestations of attributes;*
>
> *(iii) for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode;*
>
> *(vi) for interaction between two persons' European Digital Identity Wallets for the purpose of receiving, validating and sharing person identification data and electronic attestations of attributes in a secure manner;*
>
> *(viii) for relying parties to verify the authenticity and validity of European Digital Identity Wallets.*

3. Core Concepts

3.1. Description

For a legal person, a digital wallet serves as a critical tool, enabling the entity to function as an **Issuer**, **Holder**, and **Relying Party** within the digital identity ecosystem. This wallet must support a wide range of capabilities, including the issuance, retrieval, storage, and secure sharing of organisation-related information. Additionally, it must provide robust control over the data shared and requested, ensuring that sensitive business information remains secure and accessible only as intended.

User: legal person

Goal:

- Enable the legal entity to act as Issuer, Holder, and Relying Party using a digital wallet.
- Facilitate secure issuance, retrieval, storage, and sharing of company-related information.

- Maintain control over information shared and requested.

Reason:

- Securely manage attestations and data exchanges with other parties.
- Ensure privacy and control over sensitive company information in digital interactions.

3.2. Conceptual model for wallets

The **ARF** (v1.2 and v1.4) primarily focuses on the EUDIW for natural persons, emphasizing the role of the **Holder**. However, early work within the **European Wallet Consortium (EWC)** aimed to expand this perspective to address the unique requirements of legal person wallets, recognizing the differences in architecture and functionality between mobile device wallets for natural persons and server-based wallets for legal entities.

The figure below presents the conceptual model used within the EWC, illustrating the relationships between users, roles, wallet solutions, and their components. This model is intended as a high-level overview and does not describe specific technical implementations. Definitions and sources for these concepts are detailed in section 1.2 Terminology.

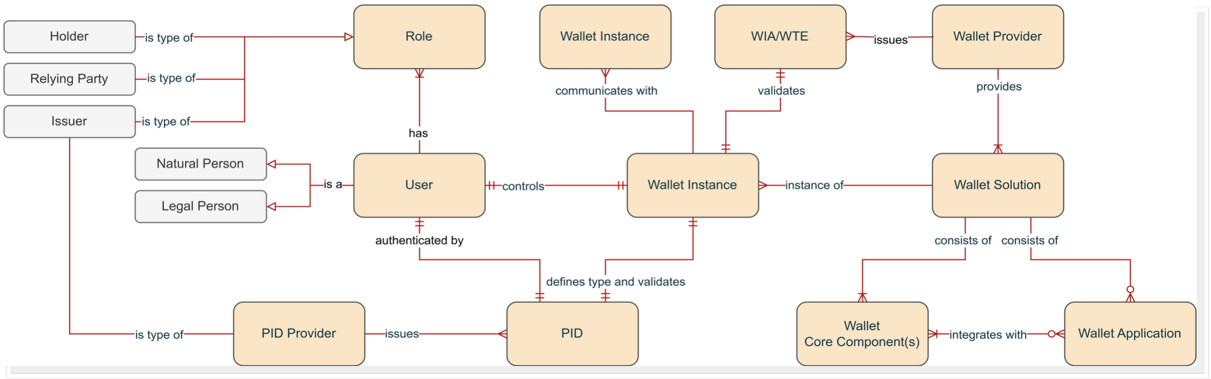


Figure 1: Conceptual model for digital identity wallets

A **wallet solution** is a technical system that must include at least one **Wallet Core Component (WCC)** and may also include a **wallet application** as an optional extension. The WCC provides the foundational functionality needed for secure communication with other wallets, while the wallet application, if present, adds end-user-facing features such as graphical interfaces and end-user authentication. Both components integrate to form a cohesive wallet solution.

Key Elements of the Model:

- **Wallet Instance:** A specific deployment of a wallet solution that communicates with other wallet instances. Each instance can be controlled by a natural or legal person, depending on the context and use case.
- **Roles:** Users can assume different roles depending on the context, acting as **Holders**, **Issuers**, or **Relying Parties**. This flexibility is essential for supporting a wide range of business interactions.

- **Authentication:** The Person Identification Data (PID) is used to authenticate users. For a wallet to be considered Valid, both the Wallet Instance Attestation (WIA) and PID must be independently validated and verified. If either the WIA or PID is missing or invalid, the wallet instance is considered either Operational (PID missing or not valid) or Installed (WIA missing or not valid).

- **Trust Foundation:** The mutual exchange of WIA and PID is the cornerstone of trust within the EUDI wallet infrastructure. This mutual validation establishes a trusted relationship between parties, ensuring secure transactions and data exchanges.

It is important to note that while the EWC has developed this conceptual model, the precise technical specifications for implementing secure, standards-compliant, and privacy-preserving solutions are still under active development. As such, this chapter focuses on the foundational concepts necessary for understanding the broader architecture, rather than the detailed technical requirements.

See the following diagram for a visual representation of the EUDIW states as described in ARF v1.4.

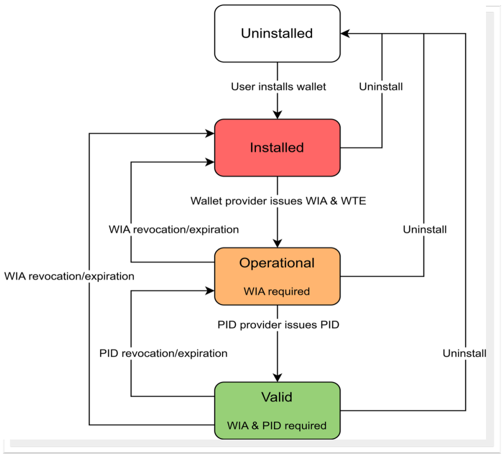


Figure 2: EUDIW state diagram

4. Basic wallet architecture

4.1. Background

The design of the European Digital Identity Wallet (EUDIW) architecture draws on concepts from the Self-Sovereign Identity (SSI) model to communicate the desired goals for both the EUDIW and its supporting trust framework infrastructure. This approach ensures a clear understanding of the roles and interactions within the digital identity ecosystem.

To describe the functionalities of the EUDIW, roles and actors from the SSI model have been adopted, including:

- **Holder** – The entity that possesses and manages digital credentials.

- **Issuer** – The entity that issues verifiable credentials.

- **Verifier (Relying Party)** – The entity that requests and validates digital credentials from a Holder.

- **Verifiable Data Registry** – The component that stores and verifies the existence and status of credentials.

Additionally, a **Revocation Registry** has been introduced to emphasize the importance of separating revocation information from the credential itself, ensuring that issuers can efficiently publish and manage the status of credentials. These roles are defined in detail in section 1.2 Terminology.

It is essential to note that users will rely on the EUDIW regardless of the capacity or role they assume. The figure below provides a visual representation of the interactions within the EUDIW ecosystem.

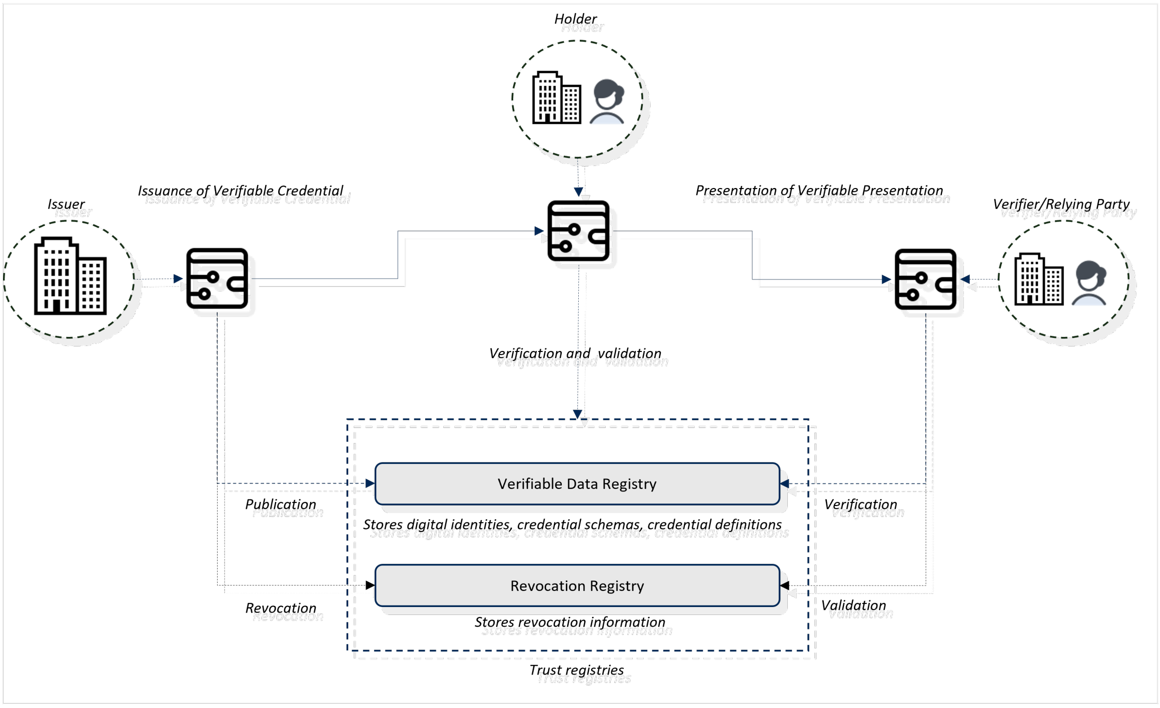

Holder
Issuer
Issuance of Verifiable Credential
Presentation of Verifiable Presentation
Verifier/Relying Party
Verification and validation
Verifiable Data Registry
Publication
Verification
Stores digital identities, credential schemas, credential definitions
Revocation Registry
Revocation
Validation
Stores revocation information
Trust registries

Figure 3: EUDIW usage per user

4.2. Roles supported by architecture

The architecture supports three primary user roles: **Issuer**, **Holder**, and **Verifier (Relying Party)**. These roles are context-dependent and determined by the nature of the transaction being performed:

- **Issuer Role** – When an entity issues credentials, it acts as an Issuer. This entity provides digital attestations about itself or its agents, including attributes such as identity, qualifications, or powers of representation (e.g., power of attorney).

- **Verifier Role** – An entity acts as a Verifier when it requests presentations from a Holder to validate identity or assess eligibility. For instance, a Relying Party may request a Portable Identity (PID) from a Holder to confirm the identity of the presenter before accepting a credential.

Co-funded by the European Union

- **Holder Role** – An entity acts as a Holder when it presents its credentials to other entities, seeking verification. This role includes validating the identities of both Issuers and Verifiers to ensure the integrity of the credential exchange process.

For a more standardised approach to credential exchanges, the architecture aligns with the OpenID4VCI specification, which **recommends**[1] that Credential Issuers dynamically request presentations of additional credentials using the OpenID4VP protocol. This allows the Issuer to act as a Verifier, creating a seamless transaction flow within the EUDIW framework.

Legal person wallets present unique requirements, as they often need to support all three roles simultaneously to accommodate organisational interactions. Key capabilities include:

- Credential issuance (e.g., corporate identity, product certifications, or delegation of authority).
- Secure storage and management of self-issued and third-party credentials.
- Robust validation mechanisms, including the ability to revoke credentials.
- End-to-end secure communication to support direct B2B interactions without human intervention.

4.3. Key components of the architecture

The architecture for legal person wallets requires additional components beyond those necessary for natural person wallets. Unlike mobile-based wallets designed primarily for end-user interaction, legal person wallets must integrate seamlessly with internal enterprise systems, often in server environments. Key components include:

- **Wallet Core Component (WCC)** – The central element that manages all essential wallet functions, including credential storage, issuance, and verification. It is crucial for maintaining secure, end-to-end communication with other wallets, regardless of the deployment model (on-premises or Wallet-as-a-Service).
- **Wallet Application (Optional)** – Provides a user-friendly graphical interface for managing attestations and credentials. This component relies on the WCC for core functionality but offers enhanced usability for end users, including:
    - Managing PIDs and (Q)EAAs;
    - Displaying and revoking attestations;
    - Facilitating user interaction through intuitive UI elements.

For server-based implementations, the architecture must support automated workflows, allowing organisations to handle credential exchanges without manual intervention. This

[1] From OID4VCI specification (draft 12), "It is RECOMMENDED that the Credential Issuer use [OpenID4VP] to dynamically request presentation of additional Credentials. From a protocol perspective, the Credential Issuer then acts as a verifier and sends a presentation request to the wallet. The Client SHOULD have these Credentials obtained prior to starting a transaction with this Credential Issuer."

includes integrating with existing systems, scheduling tasks, and managing transactions programmatically.

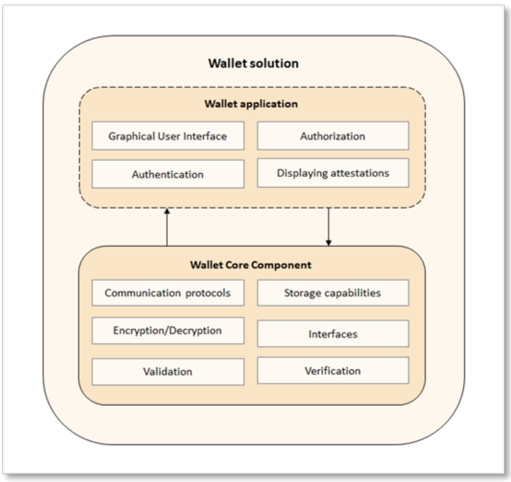


Figure 4: The wallet solution and its components: wallet core component(s) and wallet application (optional)

4.4. Requirements

For a detailed list of requirements specific to legal person wallets, refer to Annex I, which outlines key considerations identified throughout the EWC lifecycle. These requirements have guided wallet providers within EWC in their respective implementations of wallet solutions.

5. Trust infrastructures

This chapter focuses now on the special needs of the legal person wallets regarding trust infrastructures.

Unlike a natural person wallet, which typically relies on standardised and relatively uniform trust mechanisms based on authentic sources, a legal person wallet must support flexible trust frameworks tailored to different regulatory and business contexts. Such trust frameworks can leverage official registers from authentic sources, industry-specific attestations (like licenses and permits), and sector-specific third-party frameworks for example, those described in regulations such as the Digital Product Passport.

Legal Person Wallets operate often in B2B use cases, which are usually executed in a context of a business or ecosystem agreement. This means, that the eIDAS trust framework should enable extending the use of wallets to business contexts. This chapter outlines layers of trust establishment necessary for Legal Person Wallets in B2B and B2G use cases. Our expectation is that the Legal Person Wallet use cases will challenge the scalability of the eIDAS Trust Framework and Trusted List infrastructure more than the natural person use cases will. More analysis on this, is available in Annex II.

To ensure a high level of scalability, security, compliance, and interoperability, trust must be established based on following key questions: Who is the attestation provider? Is the information valid and untampered? Are the providers authorized to act in their eIDAS defined role? Are the providers authorized to act in the context of the use case? The following mechanisms are used to answer these questions:

1. Wallet Interaction enables exchange of attestations and metadata used to validate the integrity of data and verify the signatures.
2. Person identification data for legal person (LPID) is used by relying parties to identify the attestation provider.
3. eIDAS trusted lists are used to verify the authorization to act in eIDAS context
4. Use case trust infrastructures are used to verify the authorization to act in the use case context.

In EWC, we are defining these as part of Trust Mechanism RFC, which describes what verifications needs to be done and how to utilise the trust infrastructures to verify the involved parties and information.

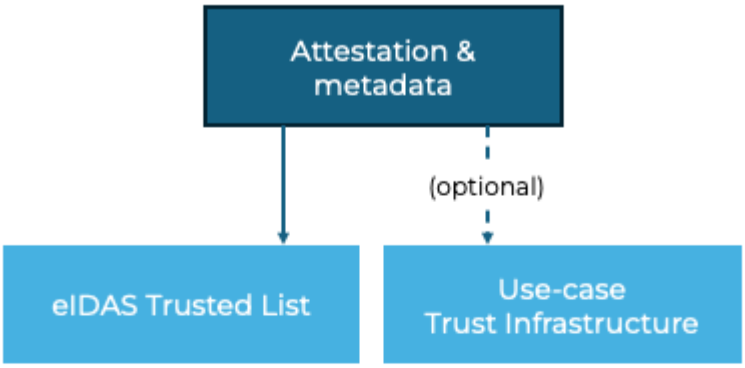


Figure 5: Trust mechanism EWC

5.1. Wallet interaction for exchanging attestations and metadata

Wallet-to-wallet interactions rely on the mutual exchange of data using standard protocols. The following information is exchanged between the wallets:

1. The attestation, which provides the information required by the business use case.
2. Contextual Metadata, which provides essential details about the attestation, the issuer, and the use case context.
3. Trust establishment information, which anchors the attestation to the trusted list and the use case specific trust infrastructure

Using the exchanged information, the verifier is able verify that the digital signatures are valid and content is not tampered with. Even more important is that the interaction sets the context for the trust infrastructure verifications happening next.

The EWC Trust Mechanism RFC details the steps and requirements for different roles.

5.2. Anchoring authority and compliance with eIDAS trust infrastructure

The eIDAS Trust Infrastructure is based on Trusted Lists, which act as an authority registry maintained by the member states. Verifying the provider information from the trusted lists guarantees that the listed providers are compliant with European regulatory standards and prevents unauthorized actors from issuing or relying on credentials.

For B2B and B2G use cases, there is little need for the Access Certificates and Registration Certificates, as business data exchange is based on agreements which define the rules of engagement. Businesses have the freedom to decide what data to request and what to provide. For this purpose, the eIDAS trust infrastructure should be used for a single purpose: verification of the authority status of the PID Providers, Wallet Providers and attestation providers. Any other authority verifications should be done using use case trust infrastructures and by providing required information using attestations.

The EUDI Wallet ecosystem requires scalability from the trust infrastructures, due to large number of ecosystem members. Equally important is responsiveness to continuous updates, due to demanding and fast paced implementation environment. In order to enable a scalable and robust trust infrastructure, we propose that Member States should be able to notify alternative trust infrastructures (e.g., distributed ledgers or federated trust networks), which are anchored in the trusted list. This model is explored in Annex II.

It is worth acknowledging that an organisational wallet may also operate in multiple regulatory frameworks, which means they will be anchored in multiple trust infrastructures. For example, an organisation's wallet may be valid according to eIDAS, but also according to other regulatory frameworks.

5.3. Binding attestation with LPID (credential chaining)

Legal person wallets should be able to issue attestations by binding the attestation directly with their identity. This is extremely useful for use cases where verification of the identity of the issuer is required. The legal person wallet can embed their Legal PID into the metadata of the issued attestation. The verifier then extracts the PID bound to the attestation and verifies the PID issuer from the trusted list, ensuring that the trust chain integrity is intact and anchoring in the eIDAS trust framework exists.

5.4. Use case-specific authority verification from a third-party trust framework

While eIDAS provides a general trust framework, attestations are often specific to business environments and require domain-specific trust infrastructures tailored to that business ecosystem. These trust infrastructures may be very different from each other in size and scope. Key technical requirements include flexible integration of multiple trust anchors to reliably verify interactions across sectors, enhancing interoperability in transactions between different regulatory frameworks. Additionally, technical specifications may be necessary to define trust anchors for systems representing organisations, enabling secure system-to-system interactions.

Examples include:

1. Supplier Networks: Large enterprises may operate internal trust registries to verify supplier compliance (e.g., Know Your Supplier - KYS).
2. Digital Product Passports: The European Green Deal mandates verifiable product lifecycle attestations, which require custom trust frameworks beyond eIDAS.
3. Payments: B2B payments could be enabled on a global scale by ensuring that existing payment infrastructures can be efficiently included.

This requires a common mechanism to anchor the use-case specific, third-party trust infrastructure to the wallet interaction. It also allows scaling the trust anchoring without disrupting the core wallet architecture.

6. Use cases for legal person wallets

6.1. Introduction

This chapter outlines four generic use cases for legal person wallets, supported by real-world examples. Unlike wallets for natural persons, legal person wallets often require integration with internal systems, eliminating the need for direct end-user interaction. These wallets, once issued with a Legal Person Identity (LPID), function as organisational wallets with the legal person as the user in control.

Legal person wallet use cases differ significantly from natural person scenarios, as they often do not involve direct human interaction. In cases where human initiation is required, organisations can implement custom client applications, such as web-based or desktop interfaces, without requiring a dedicated wallet application. When a wallet instance holds a Natural Person Identity (NPID), the user in control must be a natural person, aligning the user and end-user as the same entity.

The following sections describe use cases where the wallet solution contains only a Wallet Core Component (WCC), without the need for end-user interaction. In these cases, the legal person in control is always the organisational entity, with no natural person operating the wallet. In the figures, the organisational wallet is represented on the right-hand side to emphasize this server-based approach.

Note: All visual representations of use cases in the related images are based on protocols outlined in the ARF. While these protocols may not represent the most suited configurations for legal person use cases, they are presented here as the ARF serves as the governing framework for EWC.

The examples provided also demonstrate compliance with **Article 6a.4a**, which requires wallet solutions to support common protocols and interfaces. This alignment ensures that all WCC-based wallet solutions are interoperable, even in environments where no direct human interaction occurs.

6.2. Wallet-to-wallet interactions

1) Natural person wallet to legal person wallet

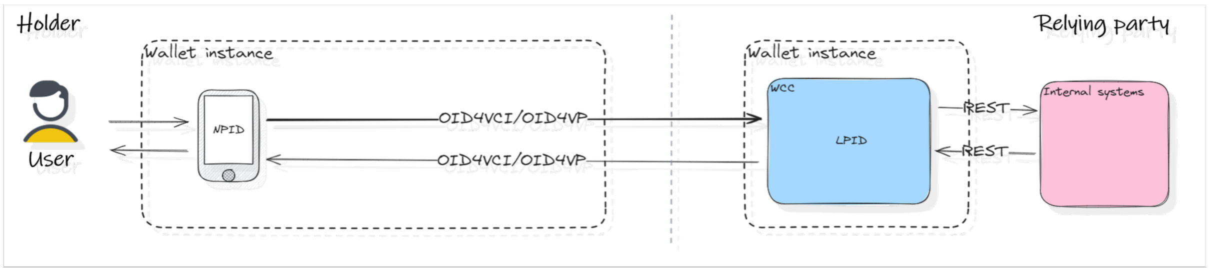
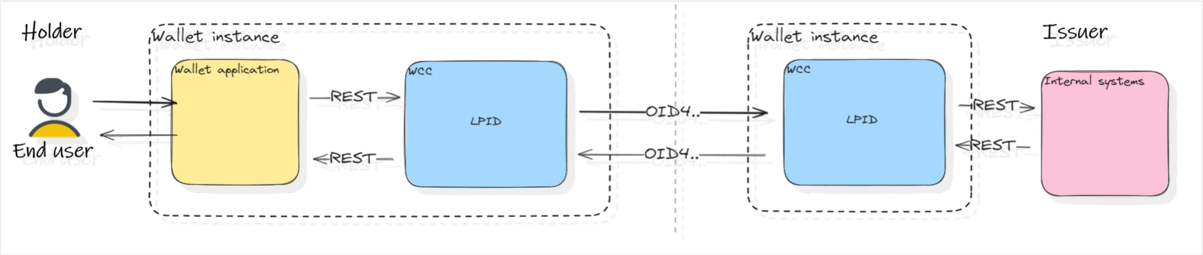


Figure 6: Communication between a natural person wallet and a legal person wallet

In the figure above, the User is also the end user and interacting with their wallet on a mobile device (left hand side). The wallet solution of the legal person is a WCC only type of solution (right hand side). The natural person wallet instance communicates with the organisational wallet instance where the user in control is a legal person and does not have an end user.

Real-world examples:

- **Online Shopping:** Hugo uses his mobile wallet to authenticate with an online retailer's organisational wallet. The retailer's WCC verifies and validates the presentation of Hugo's Portable Identity (PID) automatically, granting access without requiring manual intervention by the retailer.
- **Bank Account Creation:** Caroline uses her mobile wallet to open a bank account, sending presentations such as proof of residence. The bank's WCC handles all communication with Caroline's wallet, verifying and validating the credentials before automatically creating the account, without any bank employee involvement.
- **Car Rental:** Michelle rents a car online using her mobile wallet, presenting a digital driver's license. The car rental company's WCC verifies and validates the presentation, processes the order in its internal system, and issues a digital receipt as an attestation, all without human intervention.



2) End user operated legal person wallet-to-wallet communication

Figure 7: Communication between legal person wallets with one wallet instance operated by an end user

In this case, an end user (e.g., an employee) initiates a credential request or presentation from a wallet application, while the receiving wallet of the Issuer remains an organisational WCC without direct human control.

Real-world example:

- **SME Credential Verification:** A small or medium-sized enterprise (SME) purchases a wallet solution from a provider. An employee can request presentations from potential partners, suppliers, or buyers before signing agreements, such as product certifications, tax certifications, ownership certificates, and credit scores. These presentations are verified automatically by the WCC without manual intervention.
    - The potential partner, supplier or buyer (right hand side) also wants to verify and validate the SMEs presentations of WIA and LPID.

3) End user operated internal system with legal person wallet-to-wallet

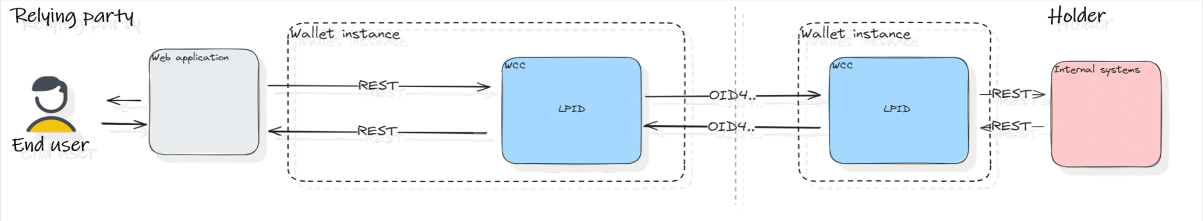
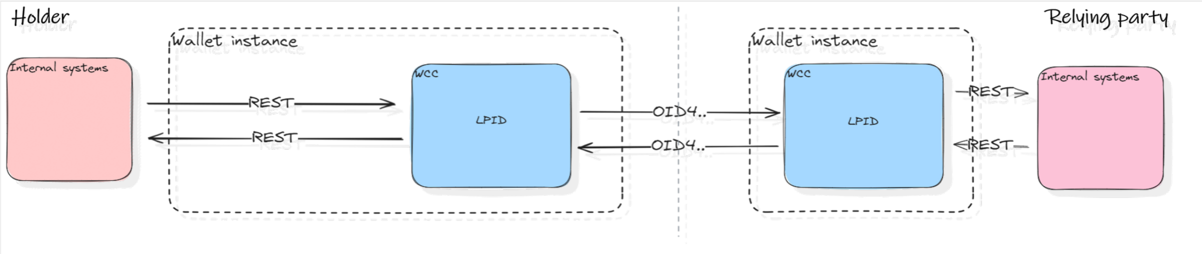


Figure 8: Organisational wallet-to-wallet communication with an end user in an internal system

This example is similar to the use case above, but this use case involves an internal web application integrated with an organisational wallet, providing a tailored user interface for business processes. This approach allows organisations to integrate their wallets with existing systems for automated transaction management.

Real-world examples:

- **Logistics Management:** An IKEA employee manages logistics partners through an internal web application, requesting safety certifications, insurance proofs, and emissions compliance from partners via the wallet. The WCC verifies and validates the presentations, enabling automated supply chain decisions.
- **Procurement Management:** A Bosch employee triggers procurement actions within an internal order system, generating automated presentation requests for suppliers. These requests, processed through the WCC, validate credentials such as registration status and product certifications before placing orders.



4) Internal system operated legal person wallet-to-wallet communication

Figure 9: Internal system controlled organisational wallet-to-wallet communication

In this purely server-to-server interaction case, internal systems trigger requests and responses without any direct human involvement, supporting fully automated credential management.

Real-world examples:

- **Automated Government Reporting:** A company's WCC periodically sends required statistics to a government agency's EUDIW, ensuring regulatory compliance through automated, scheduled reports.
- **Credential Lifecycle Management:** When a credential expires or is revoked, an issuer's internal system triggers automatic credential renewal or replacement, ensuring compliance without human intervention.

7. Patterns for wallet use

Can a Natural Person be represented in a legal person wallet? And how do we do that?

This section proposes some patterns on how to use the EUDI wallet of either a natural or a legal person to initiate a transaction for an organisation. This section does not make recommendations but shortly describes the models and use cases that fit a particular model. It is up to the relying party to analyse which of the patterns best fits their requirements and use cases and make a choice between the patterns.

While the patterns potentially fit many kinds of use scenarios, an example used here is the EU company certificate that is issued by a competent business register to the wallet of the legal or natural person and then presented, together with PID to the relying party.

7.1. Natural person wallet only

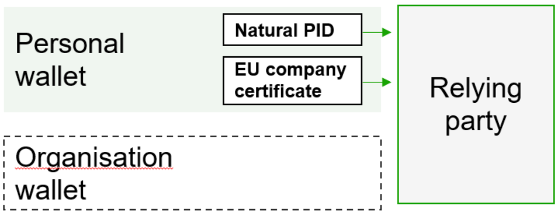


Figure 10: Natural person wallet dance

In this pattern, a natural person representing a legal person has received an EU company certificate in their natural person wallet and presents it, together with their natural PID, to the relying party. If the relying party wants to confirm the natural person's powers to represent the legal person in the transaction it can compare the PID with the list of legal representatives in the EU company certificate.

Co-funded by the European Union

7.2. Legal person wallet only

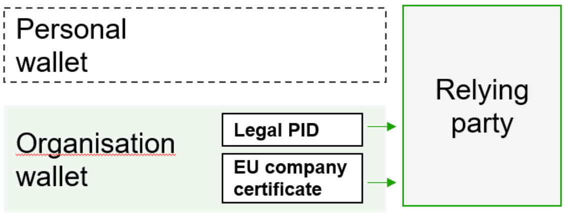


Figure 11: Legal person wallet dance

In this pattern, no natural person wallet is used. Instead, the EU company certificate is issued to the legal person wallet and presented from there to the relying party, together with the legal PID. The relying party does not learn who individual (if any) uses the legal person wallet and if they have a mandate to represent the legal person.

7.3. Both legal and natural person wallets

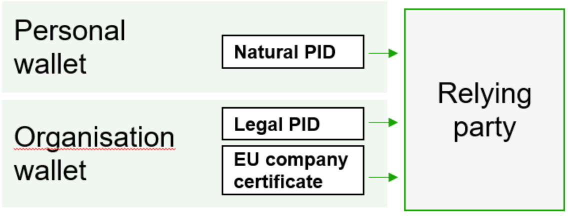


Figure 12: Combination dance

This pattern combines the two above. The natural person representing the legal person first authenticates and presents their natural PID to the relying party and indicates the legal person wallet used by the legal person they represent. The relying party then requests and receives the EU company certificate and legal PID from the legal person wallet. If the relying party wants to confirm the natural person's powers to represent the legal person in the transaction it can compare the natural PID with the list of legal representatives in the EU company certificate.

7.4. Both legal and natural person wallets and a mandate

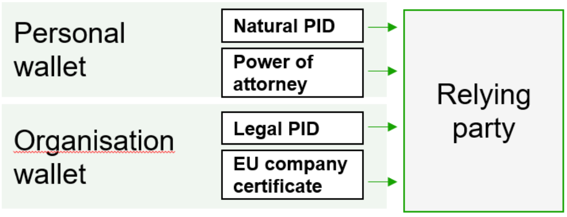


Figure 13: Combination + mandate

The natural person representing the legal person is not necessarily mentioned in the EU company certificate but has a separate mandate to act on behalf of the legal person in a particular transaction. This pattern adds to the previous one a dedicated Power of attorney attestation that the legal person issues to authorise the natural person to act on behalf of it. The mandate can be issued to and presented to the relying party either from the wallet of the natural person or the legal person. If necessary, the mandate can also be issued by a third party (e.g. QTSP provider).

8. Conclusions

This document underscores the need for a legal person digital wallet within the European Digital Identity Wallet (EUDI) framework, grounded in eIDAS2 regulations. It outlines what a legal person wallet should be capable of, including management of attestations, interaction with other wallets, and compliance legal and technical requirements. The distinction between legal person and natural person wallets is crucial, as legal person wallets often require integration with internal systems and server environments, without the need for constant end-user interaction.

A legal person wallet differs from a natural person wallet in several key areas:

- **Form Factor**: Legal person wallets are frequently deployed in server environments, such as on-premises or cloud-based infrastructures, often without a graphical user interface (GUI), whereas natural person wallets typically operate on mobile devices with a user-facing GUI.
- **Automation**: Legal person wallets are designed for automated operations, enabling interaction without an end user. Natural person wallets rely heavily on the end user for credential management.
- **Complexity of Use Cases**: Legal persons may need to integrate internal systems and processes, such as enterprise resource planning (ERP) and customer relationship management (CRM) systems, with the wallet. Natural person wallets, by contrast, are used primarily for individual credential management.
- **Credential Management and Presentation**: The ability to store, manage, and selectively present credentials is a feature. Legal persons must maintain control over which credentials are shared with external parties, while ensuring compliance with regulatory requirements.
- **Issuer and Relying Party Functionality**: Each organisational wallet must support both issuer and relying party functionalities, enabling the issuance and verification of credentials.
- **Wallet Core Component (WCC)**: The wallet must support core functionalities, including communication between different wallet instances and automated exchange of credentials.
- **Cloud Integration**: Legal person wallets must be deployable in flexible environments, supporting both on-premises and cloud-based installations. This is essential for organisations needing scalable, enterprise-level solutions that can integrate with existing systems and infrastructure.
- **Interoperability and Standards Compliance**: The wallet must be compliant with key standards and protocols defined in the implementing acts, ensuring that it can operate seamlessly with other wallets and systems across borders.

Co-funded by
the European Union

- **Security and Encryption**: Security is paramount. The wallet must implement strong encryption for both storage and communication of credentials, adhering to industry standards to protect organisational data.

By meeting these high-level requirements, the legal person wallet enables secure, trusted, and automated interactions while distinguishing itself from natural person wallets in terms of functionality and deployment.

Annex I Requirements

Annex I only states requirements on wallet solutions from a legal person perspective.

The requirements in this document are mainly focused on the functionality of the wallet core component. While all wallet providers (WP) must implement the functionality of the WCC in order to secure interoperability, trust and security, the functionality of the wallet application (WA), beyond the basic requirements, can be left to the decision of the WPs.

X and *Y* are used as placeholders in the requirements for future standards.

I.1 Wallet Application (WA) high-level requirements

Requirement ID	**Requirement**
WA_001	The wallet application SHALL allow end users to authenticate according to required level of assurance.
WA_002	The wallet application SHALL allow authenticated end users to view stored attestations.
WA_003	The wallet application SHALL allow authenticated end users to view historic information about expired and or deleted attestations.
WA_004	The wallet application SHALL offer a graphical user interface.
WA_005	The wallet application SHALL allow authenticated end users to view requested presentations.
WA_006	The wallet application SHALL allow an authenticated end user to accept or deny requests for presentations
WA_007	The wallet application SHALL allow authenticated end users to view information from a PID of an *RP* when *RP* request a presentation.
WA_008	The wallet application SHALL allow authenticated end users to view information from a PID of an *Issuer* when the authenticated end user requests an attestation.
WA_009	The wallet application SHALL display the status (*Operational*/*Valid*) of the wallet instance that requests presentations from the end user.
WA_010	The wallet application SHALL display the status (*Operational*/*Valid*) of the wallet instance that sends attestation responses.
WA_011	The wallet application SHALL allow authenticated end users to sign electronic documents.
WA_012	The wallet application SHALL integrate with the wallet core

	component, supporting at least the REST protocol.
WA_013	The wallet application SHALL be able to accept requests and or events from the wallet core component.
WA_014	The wallet application SHALL be able to send requests to the wallet core component.
WA_015	The wallet application SHALL support selective disclosure of attributes.

I.2 Wallet Core Components (WCC) core capabilities high-level requirements

Requirement ID	**Requirement**
WCC_001	The WCC SHALL automatically respond with a presentation of the PID when it is requested.
WCC _002	The WCC SHALL automatically respond with a presentation of a WTE when it is requested.
WCC _003	The WCC SHALL be able to create a presentation of an attestation automatically when the user allows it.
WCC _004	The WCC SHALL be able to create a presentation from an attestation or from selected attributes within an attestation.
WCC _005	The WCC SHALL offer storage capabilities for attestations. It SHALL be possible to use a storage bundled with the WCC or an external storage.
WCC _006	The WCC SHALL support deletion of stored attestations upon request from user.
WCC _007	The WCC SHALL be able to accept attestations without a prior request of attestation (PUSH).
WCC _008	Deleted attestations and presentations SHALL be stored in a historical log within WCC.
WCC _009	The WCC SHALL support encryption of attestations according to standards in *X*
WCC _010	The WCC SHALL offer functionality for signing/sealing of attestations.
WCC _011	The WCC SHALL be able to create an attestation in requested format based on a schema.
WCC _012	The WCC SHALL offer the possibility to publish schemas in a VDR.
WCC _013	The WCC SHALL be able to send attestations without a prior request for attestation (PUSH).
WCC _014	The WCC SHALL be able to publish revocation information in a revocation registry.
WCC _015	The WCC SHALL be able to validate received presentations.
WCC _016	The WCC SHALL offer interfaces for incoming requests.
WCC _017	The WCC SHALL as default send all events to any integrated system/wallet application.

Co-funded by
the European Union

WCC _018	The WCC SHALL offer secure storage of keys according to standard *X*.
WCC _019	The WCC SHALL support key generation according to standard *X*.
WCC _020	The WCC SHALL support communication protocols as described in *X*. Until *X* is published at least OID4VCI and OID4VP SHALL be supported.
WCC _021	The WCC SHALL support the REST protocol.
WCC _022	The WCC SHALL be able to send requests upon a request from a user.
WCC _023	It SHALL be possible to install a WCC in a server environment, cloud based and/or on-premise.
WCC _024	The WCC SHALL support integration with different VDRs. At least *X* and *Y* must be supported.
WCC _025	The WCC SHALL support auditing. All transactions SHALL be logged.
WCC _026	The WCC SHALL be able to reject attestations and presentations.
WCC _027	The WCC SHALL be able to verify received presentations.
WCC _028	The WCC SHALL be able to revalidate presentations by requests of the user.
WCC _029	The WCC SHALL support decryption of presentations according to standard *X*
WCC _030	The WCC SHALL offer storage capabilities for presentations. It SHALL be possible to use a storage bundled with the WCC or an external storage.
WCC _031	The WCC SHALL support deletion of stored presentations upon request from user.
WCC _032	The WCC SHALL support automatic acceptance of presentations upon request from the user.
WCC _033	The WCC SHALL make the status of a received presentation available to any integrated system or a wallet application.

I.3 Wallet Core Components Wallet Instance-to-Wallet Instance (WCCWI2WI) high-level requirements

Requirement ID	**Requirement**
WCCWI2WI_001	Communication between WCCs SHALL follow use the communication protocols described in standard *X*. Until *X* is published OID4VCI and OID4VP SHALL be used.
WCCWI2WI_002	Communication between WCCs SHALL be compliant with security requirements described in *X*.
WCCWI2WI_003	WCCs SHALL send attestations in formats compliant with standards described in *X*. Until *X* is published, at least SD-JWT and mDoc SHALL be supported.
WCCWI2WI_004	WCCs SHALL send presentations in formats compliant with *X*. Until *X* is published, at least SD-JWT and mDoc SHALL be supported.

Co-funded by
the European Union

WCCWI2WI_005	WCCs SHALL be able to exchange PIDs in an automated way.
WCCWI2WI_006	WCCs SHALL be able to exchange WTEs in an automated way.

I.4 Wallet Core Components External Interfaces (WCCEI) high-level requirements

Requirement ID	**Requirement**
WCCEI_001	The WCC SHALL offer an interface for requesting attestations from *Issuers*.
WCCEI_002	The WCC SHALL offer an interface for fetching one or more decrypted attestations stored in the WCC. The attestations SHALL be possible to fetch in standardised formats, at least JSON SHALL be supported.
WCCEI_003	The WCC SHALL offer an interface for fetching transaction logs stored in the WCC.
WCCEI_004	The WCC SHALL offer an interface for sending attestations to *Holders*. The interface SHALL accepts schemas as input. At least JSON SHALL be supported. The implementation of the interface SHALL create an encrypted and sealed attestation in formats defined in *X*. At least SD-JWT SHALL be supported. The attestation SHALL be sent to *Holder* without any additional steps required from the user.
WCCEI_005	The WCC SHALL offer an interface for fetching one or more decrypted presentations temporarily or permanently stored in the WCC. The presentations SHALL be possible to fetch in standardised formats, at least JSON SHALL be supported.
WCCEI_006	The WCC SHALL offer an interface for validation of presentations. The interface SHALL be implemented in such way that only the revocation information is needed for validation.
WCCEI_007	The WCC SHALL offer an interface for requesting presentations from *Holders*.

Annex II Scaling the EUDI Trust Framework

eIDAS defines the trust model that describes how trust is established in the EUDI Wallet transactions and how the trust infrastructure provided by the European Commission and Member States with the various service providers are used to validate

- EUDI Wallets;
- Wallet providers;
- Trust service providers, incl. QEAA/EAA providers and QES providers;
- Qualified Electronic Signatures;
- Providers of Person Identification Data;
- Providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source;
- Relying parties.

In addition, using electronic attestations of attributes, the wallet users can identify themselves and provide proofs attested by the attestation providers.

II.1 Trusted lists as the basis of the trust framework

The eIDAS Trust Model defines Trusted Lists as the core mechanism of the eIDAS Trust framework. Member states appoint registrars that act as the trust anchors for the EUDI Wallet ecosystem. Supervisory bodies approve entries into the trust registry after validating proper certification. The trust anchoring is described in Figure below with the following steps:

1) Each member state provides a list of registries and registrars that act as trust anchors for their respective registry;
2) Trust anchors register the providers into the member state registries;
3) Member states notify the registries to the European Commission;
4) European Commission publishes the consolidated Trusted List(s) in a machine-readable format.

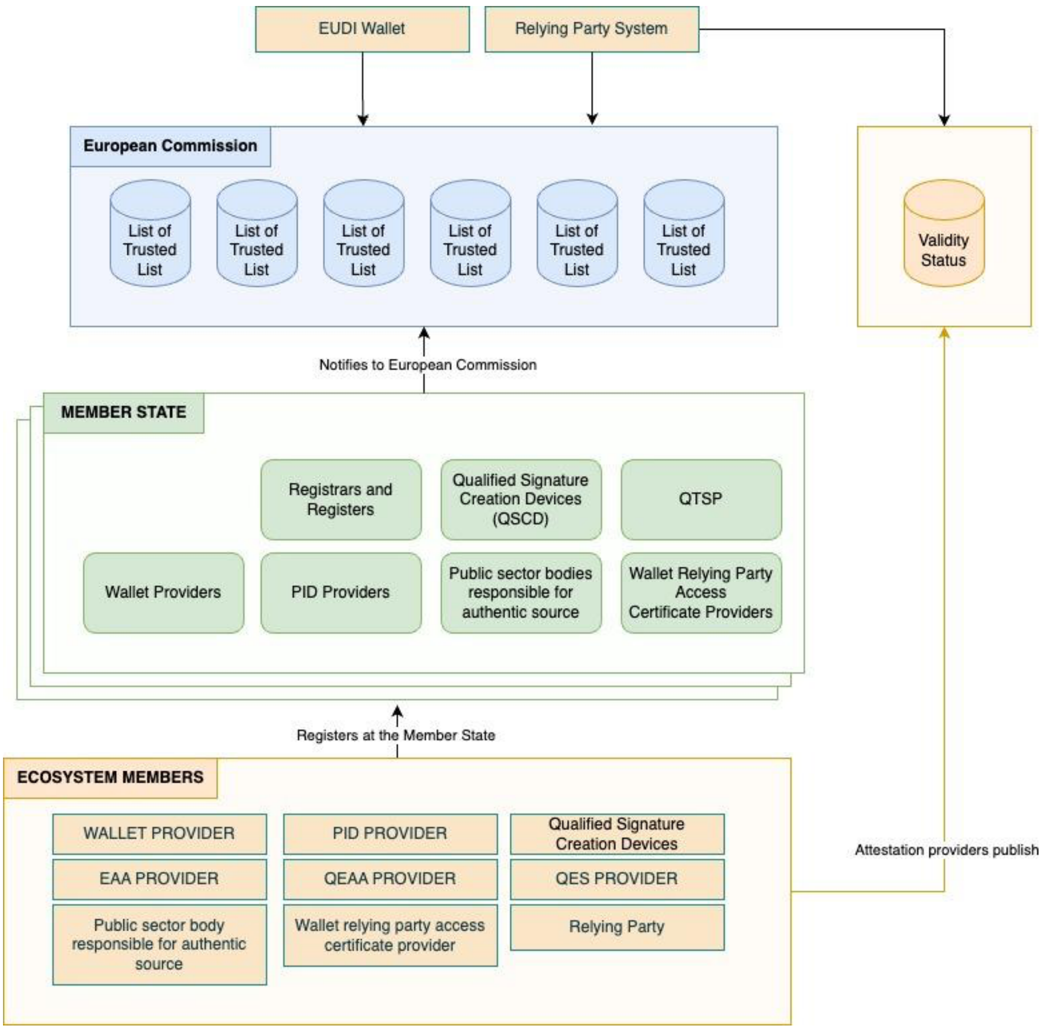

EUDI Wallet
Relying Party System
European Commission
List of Trusted List
List of Trusted List
List of Trusted List
List of Trusted List
List of Trusted List
List of Trusted List
Validity Status
Notifies to European Commission
MEMBER STATE
Registrars and Registers
Qualified Signature Creation Devices (QSCD)
QTSP
Wallet Providers
PID Providers
Public sector bodies responsible for authentic source
Wallet Relying Party Access Certificate Providers
Registers at the Member State
ECOSYSTEM MEMBERS
WALLET PROVIDER
PID PROVIDER
Qualified Signature Creation Devices
EAA PROVIDER
QEAA PROVIDER
QES PROVIDER
Public sector body responsible for authentic source
Wallet relying party access certificate provider
Relying Party
Attestation providers publish

Figure 14: High-level description of how trust anchoring works in the eIDAS Trust Model.

II.2 Scalability challenges of the Trusted List model

The Trusted List -model was originally developed to verify the authority of the trust service providers according to eIDAS v1 requirements. However, the EUDI Wallet ecosystem is considerably more complex environment than the original eIDAS ecosystem. Like identified in the earlier chapter about trust infrastructures, the trusted Lists are just one part of the trust establishment equation. However, the trust framework is only as scalable as the least scalable element.

EWC consortium members have identified, that although the Trusted List model may be suitable for anchoring a limited number of the more restricted provider types, the significant increase of entries from QEAA, Pub-EAA, PID and Wallet Providers means that the current XML-based lookup lists will likely become a bottleneck due to its size and continuous changes. Especially in the Legal Person Wallet use cases, we expect that the usage frequency is significantly higher for businesses, who get more benefits from automating the use of the wallets. Also, the total number of non-qualified providers of electronic attestation of attributes is multiple times that of the QEAA, Pub-EAA, PID and Wallet Providers together. Although EAA providers are not registered in the Trusted Lists, the wallet interaction frequency increases, pushing also demand for verifying PID Providers, Wallet Providers, QES's and other trust services from Trusted Lists.

This means that the Legal Person Wallet use cases will challenge the full scalability of the trust infrastructure more than the natural person use cases. This can be especially true for member states that have a more mature digital trust infrastructure and digitalisation rate, and where businesses will want to develop their wallet-based trust infrastructure for business-to-business use cases, increasing the need for new attestation types and providers.

Our strong opinion is that the use of Trusted Lists is not suitable for scalable trust infrastructure. Use of supplementary infrastructures must be allowed for member states that wish to utilise other trust infrastructures than the trusted list mechanism in order to support market adoption. This will be especially important for organisations wishing to utilise Legal Person Wallets in B2B use cases.

In order to support scalability and business use case adoption, we propose a supplementary approach to Trusted Lists, which enables Member States to utilise other types of trust infrastructures, such as trust registries, federation models or ledgers in addition to using the trusted list infrastructure. This infrastructure model would be more suitable for scalable and more flexible registration of providers, while anchoring it in the eIDAS Trust Model.

We acknowledge that interoperability, scalability and adoption are key requirements of the EUDI Wallet infrastructure. For this reason, our proposal is aligned with the Trusted List standards currently used by the European Commission, to mitigate any additional development needed in the standards space.

II.3 Scalable alternative to trusted lists: Member State notified Trust Infrastructures

Each Member State should be able to choose which Trust Infrastructure they use. If they choose to use a solution that is not the Trusted List compiled by the European Commission, they must notify the Trust Infrastructure to the Registries and registrars trust list.

In order to support interoperability, adoption and scalability of the EUDI Wallet ecosystem, the Trust Infrastructures must comply with the following requirements:

1) The trust infrastructures must align with the Trust Model expressed in the eIDAS regulation. This means that all trust Infrastructures must return the required cryptographic material needed to make required validations according to the eIDAS Trust Model.

2) Member state must notify the trust infrastructures to the European Commission using the Registries and Registrars Trusted List. The Registries and Registrars List of Trusted List is collected, maintained and published by the European Commission.

3) Each entry of the Trusted List of registries and registrars must include a unique identifier in the form of “Service digital identity, and an endpoint in the form of “Service supply points“, as defined in ETSI TS 119 612v2.3.1, which can be used by the relying parties to make inquiries from the registry.

4) The registered trust infrastructures must be provided either

   a. By the Member states, governed by European Commission (such as EBSI);

   b. By a member state public body;

Co-funded by the European Union

c. By an eIDAS-notified Trust Service Provider, as a Trust Service suitable for maintaining trust registry entries, such as the electronic ledger.

5) The electronic attestations of attributes must reference the trust infrastructure the provider is registered in, by using the “Service Digital identity” (see step 3). Relying parties use this identifier to validate the trust infrastructure and retrieve the service endpoint from the European Commission provided List of Trusted Lists.

6) The Trust Infrastructure must provide a harmonized interface, which is usable by EUDI Wallets and relying party software components.

7) The Trust infrastructure must provide historical information of the changes on the registered information and retain the information even after the registered entity no longer exists (e.g.: If a provider is insolvent the issued non revocable attestation still need to be verifiable by relying parties).

8) The onboarding of attestation providers to be registered in the Trust Infrastructure must be made simple so that it supports adoption and onboarding of high number of new attestation Providers. For example, use of common terms and conditions instead of individual contract negotiations should be possible, if the notifying member state supports it.

Figure below presents the high-level model of Member state notified Trust Infrastructures.

1) Member states who wish, may use the List of Trusted Lists where suitable.

2) Member states may use other Trust Infrastructures for registering providers.

3) Member State notifies European Commission of the used Registries and registrars Trusted List.

4) The Registries and Registrars Trusted List references the Trust Infrastructures that the Member States have notified.

Co-funded by
the European Union

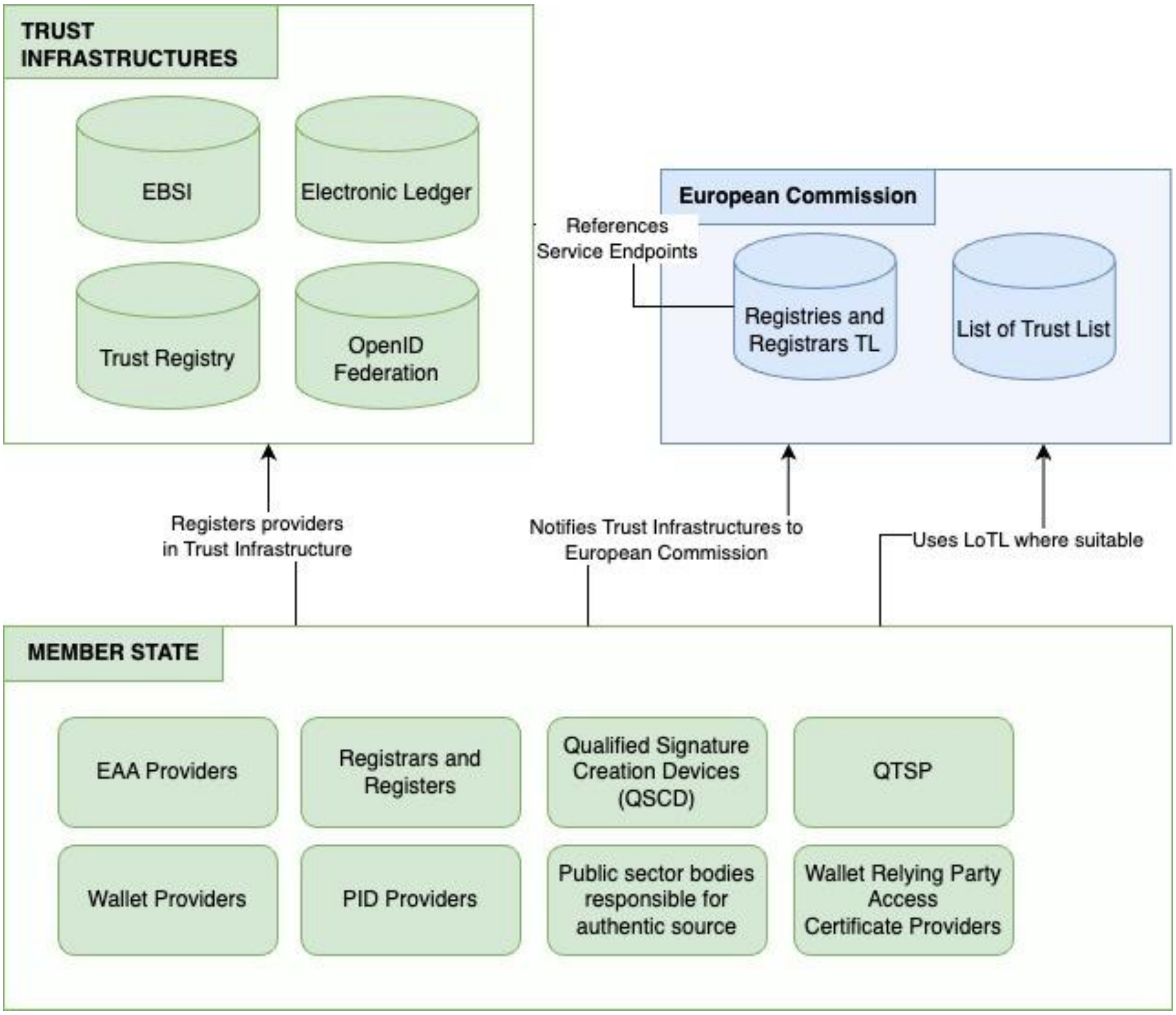

TRUST INFRASTRUCTURES
EBSI
Electronic Ledger
Trust Registry
OpenID Federation
European Commission
References Service Endpoints
Registries and Registrars TL
List of Trust List
Registers providers in Trust Infrastructure
Notifies Trust Infrastructures to European Commission
Uses LoTL where suitable
MEMBER STATE
EAA Providers
Registrars and Registers
Qualified Signature Creation Devices (QSCD)
QTSP
Wallet Providers
PID Providers
Public sector bodies responsible for authentic source
Wallet Relying Party Access Certificate Providers

Figure 15: Member state notified trust infrastructure model

II.4 Trust establishment in Legal Person Wallet interactions

II.4.1 Wallet Unit and Wallet User authentication

Interaction between two EUDI wallets is initiated by mutually authenticating the wallet units (using WUA) and wallet users (presenting PID). Figure below describes the wallet user authenticating to a relying party. Both parties will in turn act as the relying party and as wallet user to authenticate each other. This stage is always identical, no matter what the next interaction steps are (attestation issuance, presentation, etc.).

The current ARF and Implementing Acts propose the use of Wallet Relying Party Access Certificates for identification of the Relying Party, and Wallet Relying Party Registration Certificates for attesting to the registered information about the relying party.

As legal persons can already have an EUDI Wallet, they are able to perform both identification and attestation of the registration information using their EUDI Wallet. In cases where a Legal Person holds an EUDI Wallet, they should be able to identify and prove their

Co-funded by
the European Union

relying party registration information using their LPID and electronic attestations of attributes, instead of using a separate mechanism which duplicates the same capabilities.

We have understood that the concept of using certificates for authenticating the relying party is based on how ISO 18013-5 defines identification of the relying party mDL readers. Our strong opinion is that this model will unnecessarily increase redundancy, complexity and implementation costs. This is especially true for B2B use cases, where both parties in the wallet interaction already hold a wallet and can prove their identity and registration information using PID's and other attestations.

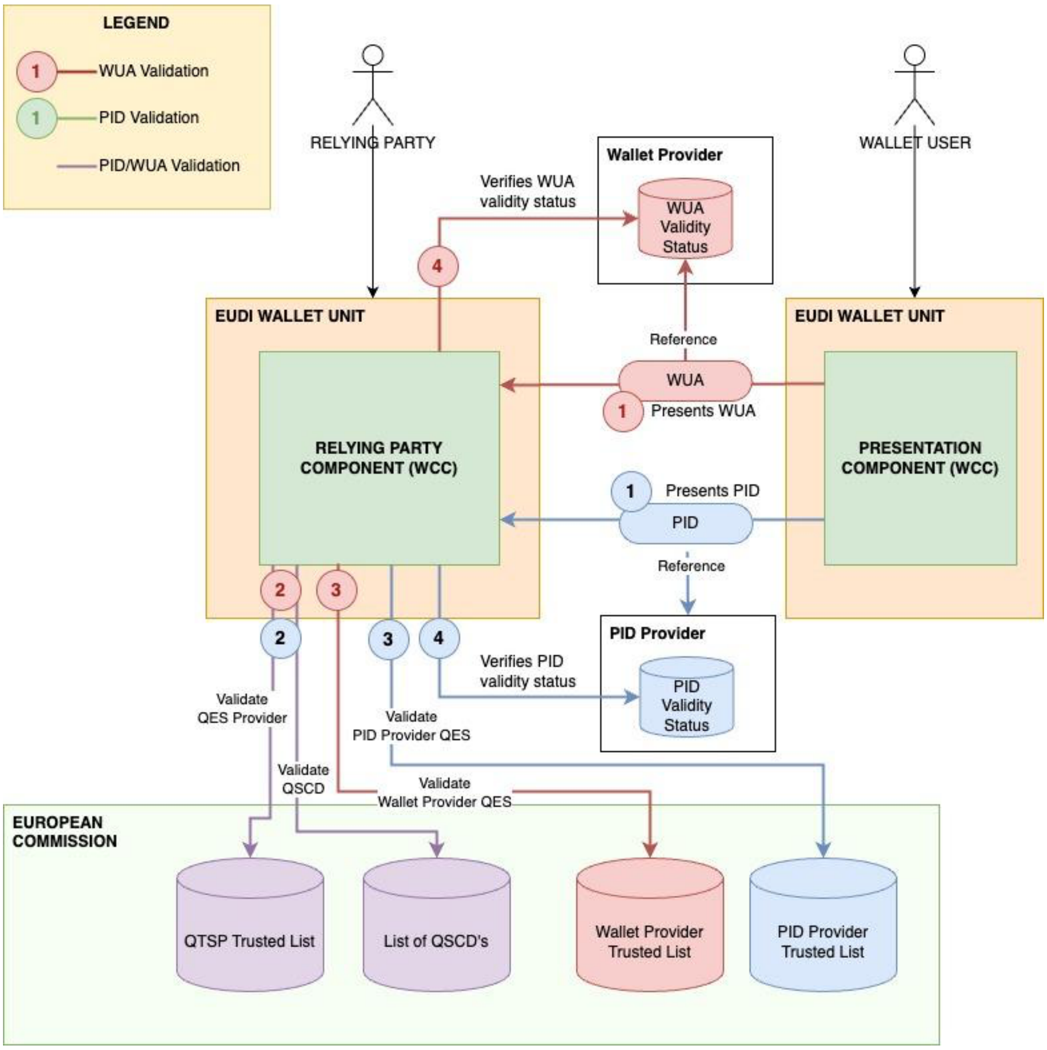


Figure 16: Wallet Unit and Wallet User authentication

II.4.2 Validation of attestations using Member State notified Trust Infrastructures

This section defines how a relying party can validate any type of attestation, when an EUDI Wallet presents an attestation provided by a provider registered in a Member State notified Trust Infrastructure.

Figure below presents the validation steps:

1) Wallet user uses the EUDI Wallet to present an attestation (named EAA but can be any type) to the Wallet Relying Party. The attestation references the Trust Infrastructure notified by the Member State to the European Commission’s Trusted List of Registries and Registrars.

2) The Relying Party uses the EC’s Trusted List to validate the Trust Infrastructure, and verify the Service endpoint of the trust infrastructure, and the registrar’s certificate to validate the signature of the registrar.

3) The relying party uses the information retrieved from the Trusted List to make a query to the member state Trust Infrastructure to retrieve cryptographic material needed to verify attestation provider.

4) If the attestation is revokable and the provider has provided location to verify the validity status, the relying party checks the validity of the attestation from the validity status location.

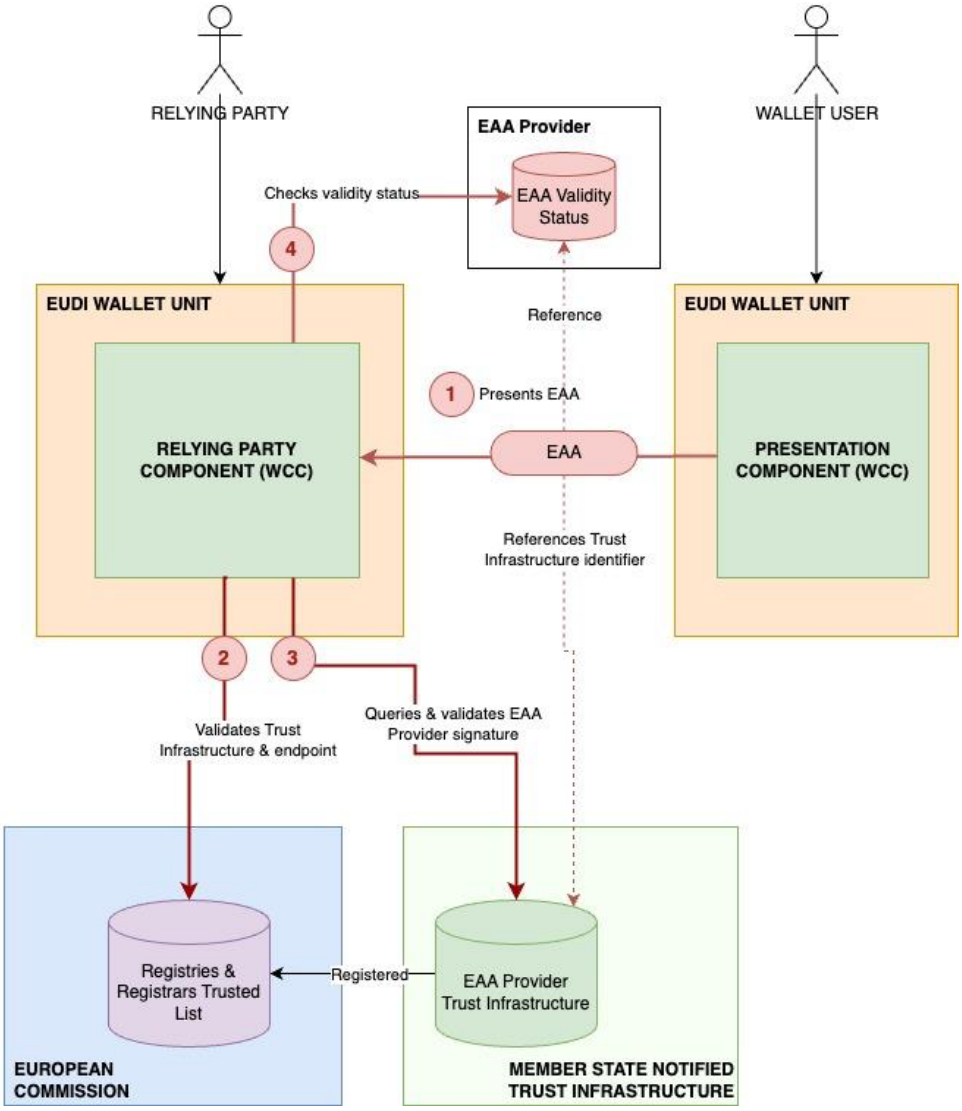

RELYING PARTY
WALLET USER
EAA Provider
EAA Validity Status
Checks validity status
4
Reference
EUDI WALLET UNIT
EUDI WALLET UNIT
1
Presents EAA
RELYING PARTY COMPONENT (WCC)
EAA
PRESENTATION COMPONENT (WCC)
References Trust Infrastructure identifier
2
3
Validates Trust Infrastructure & endpoint
Queries & validates EAA Provider signature
Registries & Registrars Trusted List
Registered
EAA Provider Trust Infrastructure
EUROPEAN COMMISSION
MEMBER STATE NOTIFIED TRUST INFRASTRUCTURE

Figure 17: Validation of attestations using Member State notified Trust Infrastructure

Co-funded by
the European Union

Using a similar model as when notifying registries and registrars of Wallet Relying Parties, as defined in Annex II of Implementing Act 2024/2980, Member States can establish their trust infrastructure. EUDI Wallets and relying parties are able to trust the Member State notified Trust Infrastructure using the Trusted List and use the infrastructure to retrieve required information for trust establishment.