# EUDI Wallet: eIDAS 2.0 and Architecture Reference Framework (ARF) v2.6.0

Guilherme Coelho
Gustavo Oliveira
Pedro Galvão

## Abstract

The European Digital Identity Wallet represents a transformative initiative in digital identity management, establishing a unified framework for secure, privacy-preserving, and interoperable identity services across the European Union. Governed by the eIDAS 2.0 Regulation (EU 2024/1183) and operationalized through the Architecture and Reference Framework (ARF) v2.6.0, the EUDI Wallet synthesizes Self-Sovereign Identity principles with institutional trust mechanisms to empower citizens with unprecedented control over their personal data. This report provides a comprehensive technical analysis of the EUDI Wallet ecosystem, examining its architectural foundations, identity management protocols, Self-Sovereign Identity alignment, organizational roles and responsibilities, and compliance with security, privacy, and interoperability standards. By combining open standards such as W3C Verifiable Credentials, ISO/IEC 18013-5, and OpenID protocols with qualified trust services under ETSI specifications, the EUDI Wallet establishes a legally binding, cross-border digital identity infrastructure. Our analysis demonstrates how privacy-enhancing technologies including selective disclosure and zero-knowledge proofs enable data minimization while maintaining high assurance levels. The report elucidates the complex interplay between user sovereignty, regulatory compliance, and technical interoperability, revealing a hybrid identity model that balances decentralization with legal enforceability. As Member States prepare for full deployment by 2026, this work provides essential guidance for understanding the technical, legal, and organizational dimensions of Europe's digital identity future.

## Keywords

European Digital Identity Wallet, eIDAS 2.0, Self-Sovereign Identity, Verifiable Credentials, Privacy-by-Design, Digital Identity, Selective Disclosure, Zero-Knowledge Proofs, Interoperability, Trust Services

## 1 Introduction

The digital transformation of European society demands a fundamental reimagining of identity management systems. Traditional approaches, characterized by fragmented national schemes, centralized identity providers, and opaque data processing practices, no longer satisfy the privacy expectations, security requirements, and mobility demands of European citizens in an increasingly interconnected digital single market. The European Digital Identity Wallet initiative addresses these challenges by establishing a unified, user-centric framework for digital identity that transcends national boundaries while respecting fundamental rights and legal diversity across Member States.

Introduced through the revision of the electronic Identification, Authentication and Trust Services Regulation—commonly known as eIDAS 2.0 (Regulation EU 2024/1183)—the EUDI Wallet represents the European Union's most ambitious digital identity project to date. Unlike its predecessor, which focused primarily on cross-border recognition of national electronic identification schemes, eIDAS 2.0 mandates that all Member States provide citizens and businesses with a personal digital identity wallet by the end of 2026. This wallet enables holders to prove their identity, store and present verified attributes, sign documents electronically, and access public and private services across Europe using a single, interoperable solution [12].

The regulatory framework establishes strict requirements for security, privacy, and interoperability while granting Member States flexibility in implementation approaches. To operationalize these requirements, the European Commission, in collaboration with Member States and stakeholders, has developed the Architecture and Reference Framework (ARF), currently at version 2.6.0. The ARF provides detailed technical specifications, protocol definitions, security requirements, and governance models that enable diverse national implementations to function as a coherent, interoperable ecosystem [1].

### 1.1 Motivation and Significance

The EUDI Wallet initiative responds to multiple converging imperatives. First, the proliferation of digital services across sectors—from e-government and healthcare to banking and e-commerce—creates mounting pressure for reliable, secure identity verification mechanisms that function seamlessly across contexts. Traditional username-password systems prove inadequate for high-assurance scenarios, while proprietary identity solutions fragment the user experience and concentrate power in the hands of large technology platforms. The EUDI Wallet offers a standards-based alternative that empowers individuals while maintaining institutional accountability.

Second, privacy concerns have intensified as surveillance capitalism, data breaches, and unauthorized tracking erode public trust in digital systems. The General Data Protection Regulation (GDPR) established strong legal protections for personal data, but technical mechanisms to enforce data minimization and user control have lagged behind regulatory ambitions. The EUDI Wallet embeds privacy-enhancing technologies directly into its architecture, enabling selective disclosure, preventing cross-service tracking, and giving users transparent control over attribute sharing [7, 8].

Third, cross-border mobility within the EU demands interoperable identity solutions. Citizens moving, studying, or working in other Member States encounter barriers when national identity documents and eID schemes are not mutually recognized. Businesses operating across borders face compliance burdens when integrating disparate identity systems. The EUDI Wallet eliminates these barriers by establishing technical and legal mechanisms for universal credential recognition, reducing friction in the digital single market [11].

Fourth, the COVID-19 pandemic accelerated digital service adoption while highlighting vulnerabilities in existing identity infrastructure. The EU Digital COVID Certificate demonstrated both the potential for rapid, large-scale deployment of verifiable credentials and the importance of privacy-preserving design. The EUDI Wallet builds on these lessons, extending the certificate's technical foundations to encompass comprehensive identity management across all sectors.

## 1.2 Self-Sovereign Identity Convergence

The EUDI Wallet represents a convergence between institutional identity systems and Self-Sovereign Identity (SSI) principles. SSI emerged from cryptographic research and decentralized systems communities as a paradigm that places individuals at the center of identity relationships, enabling them to control credential storage, manage attribute disclosure, and interact with services without intermediary gatekeepers. Core SSI concepts—verifiable credentials issued by trusted authorities, holder-controlled wallets, cryptographic proofs of possession, and selective disclosure—form the technical foundation of the EUDI architecture [4, 6].

However, the EUDI Wallet diverges from pure SSI implementations in critical ways. Unlike many blockchain-based SSI systems, the EUDI framework anchors trust through qualified trust service providers operating under regulatory supervision rather than distributed ledgers. Credentials issued within the ecosystem carry legal binding force under European law, providing assurance levels unattainable in permissionless systems. The architecture operates within a hybrid governance model that balances decentralization benefits with government-mandated compliance, strong customer authentication requirements, and sectoral regulations such as anti-money laundering directives [11].

This synthesis creates a pragmatic identity framework suited to Europe's legal, cultural, and technical landscape. It enables user sovereignty over personal data while maintaining institutional accountability. It leverages cryptographic innovation while respecting established trust mechanisms. It promotes interoperability through open standards while accommodating national diversity in implementation approaches.

## 1.3 Scope and Structure

This report provides a comprehensive technical analysis of the EUDI Wallet ecosystem, structured to address distinct yet interconnected dimensions of the framework. Section 2 examines the architectural foundations, detailing the Wallet Unit components, trust infrastructure, data exchange protocols, and design principles that ensure security, privacy, and interoperability. Section 3 analyzes the alignment with Self-Sovereign Identity principles, exploring user sovereignty, verifiable credentials, selective disclosure, privacy-enhancing technologies, and distinctions from decentralized SSI implementations.

Section 4 delineates the organizational landscape, mapping entities across user, issuance, verification, trust, certification, and governance domains, and clarifying their respective roles and responsibilities under eIDAS 2.0 and the ARF. Section 5 addresses compliance frameworks, examining security requirements including Level of Assurance High certification and cryptographic protections, privacy compliance through GDPR alignment and privacy-enhancing technologies, and interoperability compliance via adherence to W3C, ISO, IETF, and OpenID standards.

Throughout this analysis, we draw upon the ARF v2.6.0 specifications, eIDAS 2.0 regulatory texts, large-scale pilot findings, and expert commentaries to provide authoritative insights. Our goal is to furnish policymakers, implementers, researchers, and stakeholders with a rigorous understanding of the EUDI Wallet's technical architecture, legal framework, and operational implications as Europe advances toward universal digital identity by 2026.

# 2 Architectural Analysis

The European Digital Identity Wallet Architecture and Reference Framework (ARF) defines the technical and organizational foundation for a secure, interoperable, and privacy-preserving digital identity ecosystem across the European Union. It provides a modular architecture that ensures trust and interoperability among Member States while giving users full control over their digital identity credentials.

According to Sections 4.1–4.3.1 of the ARF, the system is designed around a Wallet Unit that interfaces with external entities through standardized protocols. The architecture follows key design principles such as user-centricity, security- and privacy-by-design, and cross-border interoperability, ensuring that all components interact coherently within the regulatory scope of eIDAS 2.0 (Regulation 2024/1183).

## 2.1 Design Principles

The EUDI Wallet Architecture and Reference Framework (ARF) establishes a set of core design principles that guide the development and deployment of the European Digital Identity ecosystem. These principles ensure that all architectural components — from the Wallet Unit to the trust infrastructure — operate in a consistent, secure, and interoperable manner across Member States [1].

*User-Centricity.* At the heart of the ARF is the concept of user-centricity, which prioritizes the individual's control over their identity data and credentials. Users are empowered to manage, store, and selectively disclose their digital identity attributes directly from their Wallet, ensuring transparency and autonomy in every interaction. This design choice reflects the shift towards Self-Sovereign Identity (SSI) models, where individuals, rather than institutions, own and govern their identity information.

*Privacy- and Security-by-Design.* Privacy and security are embedded as foundational architectural principles, rather than optional layers. The ARF mandates that Wallet implementations adopt strong cryptographic protections for both data at rest and in transit. Mechanisms such as secure cryptographic devices (WSCD), proof-of-possession tokens, and mutual authentication between parties mitigate risks such as impersonation, credential replay, and unauthorized access. These mechanisms align with the *privacy-by-design* obligations set forth under the General Data Protection Regulation (GDPR), ensuring that personal data processing is minimized, consent-based, and auditable [12].

*Interoperability and Standardization.* To guarantee seamless cross-border usage, the ARF relies on specific open standards it cites explicitly. In particular, it requires support for the *W3C Verifiable Credentials Data Model* for credential representation and the *ISO/IEC 18013-5:2021* mDL/mdoc model (Sec. 5.6). For protocol flows, the ARF specifies the use of OpenID for Verifiable Credential Issuance (OpenID4VCI) to handle credential issuance, and OpenID for Verifiable Presentations (OpenID4VP) to support credential presentation, as defined in Sections 5.6.1.2 and 5.6.1.3 of the ARF . For the trust layer, it references qualified certificates and trust lists under the *ETSI EN 319 4xx* family within the trust infrastructure (Chapter 6), ensuring legal assurance and cross-border recognition under eIDAS [1, 12].

*Accessibility.* According to Section 4.2.2 of the *Architecture and Reference Framework (ARF)* [1], accessibility is a fundamental design principle ensuring that the European Digital Identity Wallet (EUDI Wallet) can be used by all individuals, regardless of their abilities or specific needs. The ARF requires that Wallet implementations comply with the *Web Accessibility Directive (EU) 2016/2102* and related European standards such as *EN 301 549*, which define accessibility requirements for ICT products and services.

This principle mandates that the Wallet's user interfaces, authentication mechanisms, and onboarding procedures are designed to be perceivable, operable, understandable, and robust for users with disabilities. Accessibility considerations must be applied consistently across all device types and operational contexts, including both online and offline usage scenarios.

In practice, this ensures that every EU citizen—independent of physical, sensory, or cognitive limitations—can securely access and use their digital identity, reinforcing inclusiveness and equal participation in the digital single market.

## 2.2 Identity Management

Identity management in the EUDI ecosystem covers the full lifecycle for creating, issuing, storing, presenting, and revoking identity credentials, with the Holder in control via the Wallet Unit. The ARF defines the organisational actors, technical components, and assurance processes that together enable high-assurance, privacy-preserving digital identity across Member States [1].

*Actors and Roles.*

- **PID Provider** — Public authority (or mandated entity) that verifies civil registry data in *Authentic Sources* and issues *Person Identification Data (PID)* to the Holder's Wallet [1].
- **QEAA Provider** — Qualified Trust Service Provider (QTSP) authorised under eIDAS 2.0 to issue *Qualified Electronic Attestations of Attributes (QEAAs)* with EU-wide legal effect [12].
- **Wallet Provider / Wallet Unit** — Certified provider and Wallet components (Wallet Instance, WSCA, WSCD, backend) that securely store credentials and enforce consent, selective disclosure, and cryptographic policy [1].
- **Holder (User)** — Natural person (or legal entity representative) who controls the Wallet and decides which attributes to share, with whom, and when [1].
- **Verifier (Relying Party)** — Public or private service that requests, receives, and validates presented attributes/credentials in line with sectoral policy and level-of-assurance requirements [1].

*Credential types and sources.* **PID** are identity credentials backed by authoritative civil registers and issued by a PID Provider. **Electronic Attestations of Attributes (EAAs)** are signed statements about specific user attributes (e.g., student status, professional licence) issued by trusted entities. **QEAAs** are EAAs issued by QTSPs and enjoy the highest legal assurance under eIDAS 2.0 [12]. **Authentic Sources** are official databases (e.g., civil, vehicle, professional registers) consulted by Issuers to verify facts prior to issuance; they are not the user's Wallet storage [1].

*Identification and Authentication.* Using their Wallet Units, Users are able to:

- Identify and authenticate to online and offline services using selective disclosure and explicit approval, ensuring that only necessary, user-approved attributes are presented to Relying Parties (data minimisation) [1].
- Authenticate Relying Parties (and, where applicable, other Wallet Units) to ensure attributes are presented only to authorised and trusted entities [1].
- Onboard seamlessly with PID and (Q)EAA Providers by leveraging existing electronic identification schemes for secure registration [1].
- Be informed whether a Relying Party is authorised/registered to receive the requested attributes [1].
- Access a transaction log (dashboard) to review past interactions; request data erasure under GDPR Article 17; and report suspicious Relying Parties to the competent data protection authority [1, 12].

## 2.3 Wallet Unit Architecture

The *Wallet Unit Architecture* forms the technical core of the European Digital Identity Wallet, providing the secure environment in which users store and manage their digital credentials. According to the *Architecture and Reference Framework (ARF)* [1], the Wallet Unit defines how identity credentials and cryptographic material are structured, protected, and exchanged, ensuring security, privacy, and interoperability across all Member States.

*Main Components.* The ARF describes the Wallet Unit as a modular system composed of four tightly integrated elements that together enable secure identity management:

- **Wallet Instance** — The application installed on the user's personal device, serving as the interface for storing, managing, and presenting digital credentials. It acts as the *Holder* in the identity lifecycle and enforces consent and selective disclosure policies.
- **Wallet Secure Cryptographic Device (WSCD)** — A dedicated secure element or trusted execution environment that generates and protects cryptographic keys. The WSCD ensures that private keys never leave the secure boundary of the device and that signatures or encryption are performed in a controlled domain.

- **Wallet Secure Cryptographic Application (WSCA)** — The logical component that mediates communication between the Wallet Instance and the WSCD. It handles cryptographic operations such as key usage, digital signatures, and proof-of-possession while enforcing security and privacy policies.
- **Wallet Provider Backend** — The remote service operated by a certified Wallet Provider. It manages registration, credential lifecycle functions, and secure communication with PID and (Q)EAA Providers. Importantly, it cannot access personal data or private keys, aligning with GDPR and *privacy-by-design* principles.

*Security and Isolation Layers.* The architecture enforces a clear separation between user-facing operations and cryptographic functions. The WSCD and WSCA operate within a trusted execution environment (TEE), preventing unauthorized access or tampering. Sensitive operations such as key generation, credential binding, and digital signing occur entirely within this secure domain. This isolation embodies the ARF's *security-by-design* and *privacy-by-design* principles, ensuring that the user's credentials remain protected from device-level or network-based attacks.

*Functional Interactions.* During credential issuance or verification, the Wallet interacts with other ARF-defined entities through standardized protocols:

(1) The Wallet Instance initiates a credential issuance flow with a PID or (Q)EAA Provider using OpenID4VCI.
(2) The WSCA and WSCD perform cryptographic proof-of-possession and bind the credential to the user's secure device.
(3) The credential, following the W3C Verifiable Credential model, is stored in the Wallet Instance.
(4) When a Verifier requests validation, the Wallet presents only the necessary attributes through OpenID4VP, ensuring data minimization and explicit user consent.

*Interoperability and Compliance.* The Wallet Unit's modular architecture enables cross-border interoperability by adhering to open standards such as W3C Verifiable Credentials, OpenID4VCI, OpenID4VP, and ISO/IEC 18013-5. This ensures that Wallets developed by different Member States remain compatible while maintaining consistent levels of assurance and trust. The design aligns with the interoperability framework established under the *eIDAS 2.0 Regulation* [12], which mandates mutual recognition of digital identities and trust services throughout the European Union.

In summary, the *Wallet Unit Architecture* provides the operational foundation of the EUDI Wallet. By combining secure cryptography, privacy-preserving design, and interoperability standards, it realizes the ARF's vision of a secure, user-controlled, and cross-border digital identity ecosystem for Europe.

## 2.4 Trust Services

Trust services form the foundation of the EUDI ecosystem's trust and legal assurance layer. According to the *Architecture and Reference Framework (ARF)* [1], these services are delivered by *Qualified Trust Service Providers (QTSPs)* as defined under *eIDAS 2.0* [12]. QTSPs are responsible for issuing and managing trust elements such as qualified certificates, electronic signatures, seals, timestamps, and electronic attestations of attributes (QEAAs). These mechanisms ensure authenticity, integrity, and non-repudiation across all digital interactions within the EUDI Wallet ecosystem.

The ARF (Chapter 6) establishes a dedicated *Trust Infrastructure* that connects Wallet Providers, PID Providers, and (Q)EAA Providers through certified and traceable trust anchors. This infrastructure uses qualified certificates conforming to the *ETSI EN 319 4xx* family of standards to guarantee cryptographic binding, certificate validation, and cross-border recognition. Each trust service must be registered in the EU Trusted List (EUTL), enabling automatic verification of certificates and signatures by Wallets and Verifiers.

Within the Wallet Unit, trust services support critical functionalities including identity attestation, digital signing, and validation of credentials. The ARF requires that Qualified Electronic Signatures (QES) and Qualified Electronic Seals (QSeal) be supported, ensuring that documents or credentials signed through the Wallet carry the same legal effect as handwritten signatures across all Member States. Time-stamping services provide verifiable proof of when a transaction or attestation occurred, complementing the integrity guarantees of qualified certificates.

Together, these trust mechanisms enable the Wallet to operate within a unified European trust framework, ensuring that any credential, signature, or attestation issued under eIDAS 2.0 is legally recognized and technically verifiable throughout the EU. This alignment with the ETSI and eIDAS standards provides the foundation for mutual trust, legal certainty, and secure cross-border interoperability within the European Digital Identity ecosystem.

## 2.5 Data Exchange Protocols

The *Architecture and Reference Framework (ARF)* [1] defines standardized data exchange protocols to ensure secure, interoperable, and privacy-preserving communication between the Wallet Unit and external entities such as PID Providers, (Qualified) EAA Providers, Verifiers, and other Wallets. These interactions are based on open protocols explicitly mentioned in the ARF, namely *OpenID for Verifiable Credential Issuance (OpenID4VCI)* for credential issuance (Sec. 5.6.1.2) and *OpenID for Verifiable Presentations (OpenID4VP)* for credential presentation (Sec. 5.6.1.3). Both protocols build upon the OAuth 2.0 and OpenID Connect frameworks to provide standardized, secure, and interoperable exchanges of verifiable credentials.

For proximity and offline scenarios, the ARF specifies the use of *ISO/IEC 18013-5:2021* [1], which defines the mobile document (*mdoc*) model for secure local credential presentation over interfaces such as NFC, BLE, or QR codes. These mechanisms enable the Wallet to operate even when network connectivity is unavailable, ensuring usability across all environments. All credential exchanges—whether online or offline—must ensure end-to-end confidentiality, integrity, and authenticity through cryptographic protections and mutual authentication between the involved entities.

The ARF also mandates that data exchanges comply with principles of user consent and data minimisation. Each transmission of attributes or credentials must be explicitly approved by the Holder through the Wallet interface, ensuring that only necessary information is shared with Relying Parties. This aligns with the privacy-by-design and GDPR compliance principles established under eIDAS 2.0 [12]. Together, these protocol requirements guarantee secure and interoperable data flows across all Member States, supporting both cross-border trust and user sovereignty in the European Digital Identity ecosystem.

### 2.6 Summary

The *Architectural Analysis* of the European Digital Identity Wallet demonstrates how the *Architecture and Reference Framework (ARF)* integrates security, interoperability, and user empowerment into a cohesive ecosystem governed by *eIDAS 2.0*. Each architectural layer—from identity management and trust services to data exchange protocols—contributes to a unified model of digital identity that is verifiable, privacy-preserving, and legally enforceable across all Member States.

By combining open standards such as the W3C Verifiable Credentials, ISO/IEC 18013-5, and OpenID4VCI/4VP protocols with qualified trust services under the *ETSI EN 319 4xx* standards, the ARF establishes a harmonised foundation for secure credential issuance, authentication, and validation. This architecture embodies the convergence of *Self-Sovereign Identity (SSI)* principles with institutional trust, ensuring that European citizens retain sovereignty over their personal data while benefiting from legally recognised and interoperable digital identities [1, 12].

In essence, the EUDI Wallet represents a hybrid identity framework: technically decentralised yet legally anchored, user-centric yet institutionally verifiable. It operationalises the vision of the European Union's digital single market—where trust, privacy, and interoperability coexist under a common regulatory and technological architecture.

## 3 Self-Sovereign Principles

Self-Sovereign Identity (SSI) represents a paradigm shift in digital identity management, placing individuals at the centre of control over their personal data. Unlike traditional centralised systems where identity providers hold and assert credentials on behalf of users, SSI enables individuals to maintain their own cryptographically signed attestations and selectively reveal attributes when interacting with services. The European Digital Identity (EUDI) Wallet adapts these foundational SSI principles within a legally binding regulatory framework to meet the requirements of eIDAS 2.0 (Regulation 2024/1183). This section examines how the EUDI Wallet implements core SSI concepts: user sovereignty, verifiable credentials, selective disclosure, and privacy-enhancing techniques. It also highlights the architectural and governance differences that distinguish the EUDI Wallet from decentralised SSI implementations.

### 3.1 User Control and Data Sovereignty

The principle of user sovereignty, whereby individuals control the storage, management, and disclosure of their identity data, distinguishes SSI from traditional identity systems. In the EUDI ecosystem, credentials reside on the user's device rather than in centralised registries, and explicit consent is required before any attribute is shared with a relying party [7, 8]. Citizens may request, select, store, delete, and share identity data at their discretion, and the wallet architecture prevents both issuers and verifiers from tracking user behaviour across transactions [8].

Independent analyses confirm that the EUDI Wallet grants users complete control over their credentials, allowing them to decide what information to reveal, with whom, and when [6, 10]. This decentralised storage model ensures that personal data sovereignty remains with the holder rather than service providers. Under eIDAS 2.0, every Member State must provide at least one EUDI Wallet solution enabling citizens to access public and private services using their own verifiable credentials [4]. These provisions institutionalise data sovereignty as a fundamental right within the European digital identity ecosystem.

### 3.2 Verifiable Credentials and Trust Frameworks

The SSI model operates on a three-party trust relationship: issuers create digitally signed credentials, holders store them in their wallets, and verifiers accept cryptographic proofs of credential possession. The EUDI Architecture and Reference Framework (ARF) adopts this structure through Person Identification Data (PID) and Electronic Attestations of Attributes (EAAs), which are issued by qualified trust service providers under eIDAS 2.0 [4]. These attestations are cryptographically bound to the holder through device keys and can be independently verified without contacting the issuer.

Trust in this ecosystem is anchored through trust registries that allow verifiers to retrieve issuer metadata and validate certificate status, thereby supporting cross-border credential recognition [4, 11]. Crucially, the ARF does not mandate distributed ledger technologies. Instead, it relies on qualified trust service providers and public-private governance arrangements to establish trust [11]. This approach distinguishes the EUDI Wallet from many blockchain-based SSI systems while maintaining the core verification benefits of cryptographically signed credentials.

### 3.3 Selective Disclosure and Privacy-Enhancing Techniques

Data minimisation, the practice of disclosing only the attributes necessary for a given transaction, is a cornerstone of SSI privacy protection. The ARF explicitly defines selective disclosure as the capability for the wallet to present a subset of user attributes from PID or EAA attestations [3]. High-level requirements mandate that all PID and EAA credentials support selective disclosure through privacy-preserving formats such as selective-disclosure JSON Web Tokens (SD-JWT) or mobile security objects [3].

In practice, when a verifier requests proof of a specific attribute, the wallet constructs a presentation containing only the requested data. For example, a merchant can verify that a customer is over 18 years old without learning the customer's name, date of birth, or address [5, 10]. This capability reduces both privacy risks and fraud exposure while maintaining regulatory compliance.

The discussion on zero-knowledge proofs within the ARF emphasises the importance of privacy-preserving technologies that enable validators to confirm statements without accessing underlying personal data [9]. Recital 59 of the regulation specifically calls for techniques like zero-knowledge proofs to validate claims while preserving privacy, and Article 5a mandates that wallets prevent correlation of presentations across different services [8, 9]. These technical measures, combined with architectural requirements for unlinkability, ensure that data minimisation and privacy-by-design are embedded throughout the system [2].

### 3.4 Interoperability and Security

The EUDI Wallet architecture is guided by four foundational principles: user-centricity, interoperability, privacy by design, and security by design [10]. User-centricity ensures that holders retain the authority to decide which credentials to present and may revoke consent at any time [2, 10]. Transparency regarding data sharing (what is shared, with whom, and for what purpose) is maintained throughout each transaction.

Interoperability is achieved through adherence to open standards such as OpenID Connect for verifiable presentations and the W3C verifiable credentials data model, combined with legal mechanisms under eIDAS 2.0 that ensure cross-border recognition of credentials and trust services [11]. This standardisation enables seamless interaction between national and sectoral systems across the European Union.

Privacy by design is operationalised through selective disclosure, zero-knowledge proofs, and architectural safeguards against tracking and linkability [2, 8]. Security by design integrates strong authentication mechanisms, including multi-factor authentication, secure hardware for cryptographic key storage, and rigorous protocols for credential protection [2, 10]. Together, these principles adapt SSI concepts to a high-assurance, legally compliant framework that balances decentralisation with regulatory oversight.

### 3.5 Differences from Decentralised SSI Implementations

Although the EUDI Wallet incorporates core SSI principles, it diverges from pure decentralised identity systems in several significant ways. The eIDAS 2.0 architecture does not require blockchain or distributed ledger technologies; trust is instead anchored via qualified trust service providers operating under regulatory supervision [11]. Credentials and electronic signatures issued within the EUDI ecosystem carry legal binding force under European law, providing a level of assurance not typically present in permissionless blockchain-based systems.

Furthermore, the EUDI Wallet operates within a hybrid public-private governance framework that balances the decentralisation benefits of SSI with government-mandated assurance levels and compliance requirements, including strong customer authentication under the Payment Services Directive (PSD2) [11]. Standardised protocols and attestation formats ensure both interoperability and legal recognition. These architectural choices reflect a pragmatic adaptation of SSI principles to the regulatory and operational requirements of a continent-wide digital identity infrastructure.

### 3.6 Summary

The EUDI Wallet represents a synthesis of SSI principles and regulatory compliance, embedding user control, verifiable attestations, selective disclosure, and privacy-enhancing cryptography within a unified legal framework. By combining privacy-preserving techniques with trust registries and qualified service providers, the ARF enables European citizens to prove identity attributes across borders while maintaining sovereignty over their personal information [1, 12]. The result is a hybrid identity system that empowers individuals, protects privacy, and fosters cross-border interoperability within the EU's digital single market.

## 4 Roles and Responsibilities of Entities

The European Digital Identity Wallet Ecosystem (Echosystem) is composed of various entities that play crucial roles in the functioning and management of the digital identity system. These entities include Users, Issuers, Providers, and Supervisory and Oversight Authorities. Each entity has specific roles and responsibilities that ensure the proper operation of the system while adhering to established regulations and standards. In this section, we will take a deeper look at the different entities, their roles, and their responsibilities within the EUDI Wallet Ecosystem.

### 4.1 Entities

Entities, are moustly organizations, that participate in the EUDI Wallet Ecosystem by providing services, issuing credentials, or overseeing compliance with regulations. According to the European Digital Identity Wallet Architecture and Reference Framework (ARF v2.6.0) [1], we have almoust 20 diferent entities ivolved in the Ecosystem, but we will divide them in User, Issuer, Providers and Supervisory and Oversight Authority for simplification purposes when later we talk about rulles and responsibilities.

- **User Domain**
  - **User of Wallet Unit (UoW):** The natural or legal person to whom a Wallet Unit is issued and who uses it to store, manage, and present digital credentials under their control.
- **Wallet Provisioning and Operation**
  - **Wallet Provider (WP):** An organization that develops, deploys, and maintains Wallet Units in compliance with the ARF's security, privacy, and interoperability requirements.
  - **Device Manufacturer and Related Subsystems Provider (DMRSP):** Manufacturer or supplier of secure hardware, Secure Elements (SE), Trusted Execution Environments (TEE), and related components used within Wallet Units.
- **Issuance and Attribute Provisioning**
  - **Person Identification Data Provider (PIDP):** Entity authorized to issue Person Identification Data (PID) credentials based on verified identity data from authoritative registers.
  - **Qualified Electronic Attestation of Attributes Provider (QEAA-P):** Qualified trust service provider issuing Qualified Electronic Attestations of Attributes (QEAAs) under eIDAS 2.0 [12], and ARF governance.
  - **Electronic Attestation of Attributes Provider (EAA-P):** Provider issuing non-qualified Electronic Attestations of Attributes (EAAs) in line with ARF interoperability specifications.
  - **Public Sector EAA Provider (PuB-EAA-P):** Public authority or delegated entity issuing EAAs based

  on authentic government registers or administrative databases.
  - **Authentic Source (AS):** Authoritative registry or database (e.g., population, tax, vehicle, education) holding verified identity or attribute data used by issuers.
- **Relying and Verifying Parties**
  - **Relying Party (RP):** Public or private entity that requests, receives, and verifies credentials or attributes from Wallet Users to provide access or services.
  - **Access Certificate Authority (ACA):** Authority that issues and manages digital certificates used for mutual authentication between Wallets, Providers, and Relying Parties.
- **Trust and Conformity Infrastructure**
  - **Registrar (REG):** Entity responsible for managing registries, identifiers, and metadata for participants to ensure technical discoverability and resolution.
  - **Provider of Registration Certificates (PRC):** Entity that issues registration certificates binding organizational or technical identities to registered participants in the EUDI ecosystem.
- **Technical Certification and Evaluation**
  - **Conformity Assessment Body (CAB):** Independent, accredited organization that evaluates Wallets, Providers, and components for compliance with the ARF and applicable standards.
  - **Attestation Scheme Provider (ASP):** Entity that defines evaluation and attestation schemes, assurance levels, and certification criteria for use by CABs and accreditation bodies.
- **Supervisory and Accreditation Authorities**
  - **Supervisory Body (SB):** National authority overseeing Wallet Providers, PID Providers, and Attribute Providers to ensure regulatory compliance under eIDAS 2.0.
  - **National Accreditation Body (NAB):** National authority accrediting CABs and ensuring the competence, impartiality, and consistency of conformity assessments.
  - **Trusted List Provider (TLP):** Entity maintaining and publishing trusted lists of qualified and supervised services for discoverability and trust verification.
- **European Governance**
  - **European Commission (EC):** The EU executive institution responsible for maintaining the EUDI Toolbox and ARF, ensuring policy coherence, interoperability, and governance of the entire ecosystem.

## 4.2 Roles

Each entity plays a specific role within the EUDI Wallet Ecosystem, contributing to its overall functionality and governance. In this section we will take a deeper look focused on the main entities, dividing them in User, Issuer, Provider, Trust, Governance and Supervisory roles. The Roles are well defined in de EUDI Architecture and Reference Framework (ARF v2.6.0) [1]. The following roles are defined for each entity:

- **User Role:**
  - Manage and control personal digital identity credentials stored in the Wallet Unit.
  - Provide consent for data sharing with Relying Parties.
  - Authenticate to access services using the Wallet.
- **Issuer Roles:**
  - Verify user identities and issue Person Identification Data (PID) credentials.
  - Issue Electronic Attestations of Attributes (EAAs) based on verified data from authentic sources.
  - Ensure compliance with ARF standards during issuance processes.
- **Provider Roles:**
  - Develop, deploy, and maintain Wallet Units in accordance with ARF requirements.
  - Implement strong authentication and security measures for Wallet access.
  - Ensure interoperability with other ecosystem entities.
- **Trust Roles:**
  - Manage trust registries and metadata for ecosystem participants.
  - Issue and manage access certificates for mutual authentication.
  - Facilitate cross-border trust verification among Member States.
- **Governance Roles:**
  - Maintain the EUDI Toolbox and ARF to ensure policy coherence.
  - Oversee ecosystem governance and compliance across Member States.
  - Promote interoperability and standardization within the ecosystem.
- **Supervisory Roles:**
  - Monitor compliance of Wallet Providers and Issuers with regulatory requirements.
  - Accredit Conformity Assessment Bodies (CABs) for technical evaluations.
  - Publish trusted lists of qualified services for discoverability and trust verification.

## 4.3 Responsibilities

Each entity has legally binding responsibilities under the eIDAS 2.0 [12] proposal and ARF v2.6.0 [1] to ensure the secure, interoperable, and privacy-preserving operation of the EUDI Wallet Ecosystem.: Here we look a to them the same way as in Rules, dividing them in User, Issuer, Provider, Trust, Governance and Supervisory responsibilities.

This framework has defined responsibilities for each entity to ensure accountability and compliance with regulatory requirements.

- **User Responsibilities:**
  - Safeguard Wallet credentials and private keys.
  - Provide accurate information during identity proofing.
  - Manage consent for data sharing with Relying Parties.
- **Issuer Responsibilities:**
  - Verify user identities before issuing credentials.
  - Ensure credentials comply with ARF standards.

  - Maintain secure issuance processes.
- **Provider Responsibilities:**
  - Develop and maintain secure Wallet Units.
  - Implement strong authentication mechanisms.
  - Ensure interoperability with other ecosystem entities.
- **Trust Responsibilities:**
  - Manage trust registries and metadata.
  - Issue and manage access certificates.
  - Facilitate cross-border trust verification.
- **Governance Responsibilities:**
  - Maintain the EUDI Toolbox and ARF.
  - Ensure policy coherence across Member States.
  - Oversee ecosystem governance and compliance.
- **Supervisory Responsibilities:**
  - Monitor compliance of Wallet Providers and Issuers.
  - Accredit Conformity Assessment Bodies.
  - Publish trusted lists of qualified services.

## 4.4 Summary

The European Digital Identity Wallet Ecosystem is a complex network of entities, each with specific roles and responsibilities that ensure the secure, interoperable, and privacy-preserving operation of the system. Users manage their digital identities and provide consent for data sharing, while Issuers verify identities and issue credentials in compliance with established standards. Issuers include Person Identification Data Providers and Electronic Attestation of Attributes Providers, who ensure that credentials are issued based on verified data from authentic sources. Providers develop and maintain Wallet Units, implementing robust security measures to protect user data. Supervisory Authorities monitor compliance and accredit Conformity Assessment Bodies to maintain trust within the ecosystem. Then the European Commission oversees the governance of the ecosystem, ensuring policy coherence and promoting interoperability across Member States.

This eudi 2.0 and ARF v2.6.0 framework establishes clear accountability for each entity, fostering a trustworthy digital identity environment that empowers users while adhering to regulatory requirements.

Only through the collaborative efforts of all entities can the EUDI Wallet Ecosystem achieve its goals of security, privacy, and interoperability, ultimately providing a seamless and user-centric digital identity experience for citizens and businesses across Europe.

# 5 Compliance with Security, Privacy, and Interoperability

The European Digital Identity Wallet operates within a comprehensive regulatory framework mandating strict compliance with security, privacy, and interoperability standards. The eIDAS 2.0 Regulation (EU 2024/1183) establishes legally binding requirements harmonizing digital identity services across all Member States while ensuring the highest levels of protection for citizens' personal data and cryptographic assets [12]. This section examines how the EUDI Wallet architecture achieves compliance with three fundamental regulatory pillars: security requirements protecting against sophisticated attacks, privacy regulations safeguarding fundamental rights under the General Data Protection Regulation (GDPR), and interoperability standards enabling seamless cross-border credential recognition throughout the European Union. Together, these compliance frameworks form the foundation of a trustworthy digital identity ecosystem balancing innovation with robust legal safeguards.

## 5.1 Security Compliance

*5.1.1 Level of Assurance Requirements.* The EUDI Wallet must achieve and maintain a high Level of Assurance (LoA High) for electronic identification, representing the most stringent security tier defined under eIDAS 2.0. This assurance level requires the wallet to demonstrate resistance against attackers with high attack potential, ensuring authentication and identification processes meet confidence thresholds necessary for sensitive transactions such as border control, financial services, and access to confidential government systems. Article 8 of the original eIDAS Regulation establishes three levels of assurance—low, substantial, and high—each corresponding to different degrees of confidence in the claimed or asserted identity. The EUDI Wallet targets LoA High to maximize both security and legal recognition across all use cases and Member States.

Achieving LoA High involves satisfying two distinct requirement categories. First, procedural requirements govern enrollment, authentication, and lifecycle management processes for digital identities, including identity proofing standards, credential issuance protocols, and mechanisms for revocation and renewal. Second, technical requirements relate to the robustness of electronic identification means themselves, encompassing cryptographic strength, secure key management, and protection against both logical and physical attacks. The ARF mandates that Wallet Instances interface with certified Wallet Secure Cryptographic Devices (WSCD) and Wallet Secure Cryptographic Applications (WSCA) to ensure cryptographic operations meet LoA High standards [1]. These components must undergo rigorous certification processes, often leveraging Common Criteria methodologies, to verify resistance to sophisticated threat actors.

*5.1.2 Certification and Assessment.* Member States must establish national certification schemes evaluating Wallet Solutions and electronic identification schemes under which they operate. Commission Implementing Regulation (EU) 2024/2981, adopted in November 2024, specifies functional, cybersecurity, and data protection standards wallets must meet to ensure secure and interoperable digital identity solutions. Certification schemes must address the complete wallet architecture, including software components with their settings and configurations, as well as hardware components and platforms when directly provided or relied upon for critical operations.

Certification at LoA High requires vulnerability assessments aligned with Common Criteria evaluation methodologies, specifically targeting AVA_VAN.5 pursuant to Common Criteria standards. This assessment level ensures the wallet can withstand attacks from adversaries possessing high attack potential, including nation-state actors and sophisticated cybercriminal organizations. The WSCD, responsible for managing cryptographic secrets such as private keys, must be certified under Common Criteria to provide a strong foundation for securing sensitive cryptographic operations. Many implementations leverage Secure Elements (SE) certified at

Evaluation Assurance Level 4+ (EAL4+ with AVA_VAN.5), widely deployed in modern smartphones with proven track records in securing sensitive applications like payment cards and national identity documents.

The certification process mandates regular vulnerability assessments and audits to maintain security integrity over time. Conformity Assessment Bodies (CABs), accredited by National Accreditation Bodies under Regulation (EC) No 765/2008, perform independent evaluations of Wallet Solutions. These assessments verify compliance with established security requirements, including resistance to known attack vectors, secure lifecycle management from manufacturing through retirement, and adherence to cybersecurity objectives defined in Article 51 of Regulation (EU) 2019/881 (the Cybersecurity Act). Furthermore, the European Union Agency for Cybersecurity (ENISA) is developing a harmonized European cybersecurity certification scheme for EUDI Wallets under the Cybersecurity Act, which will eventually replace national schemes to ensure consistent security standards across the EU.

*5.1.3 Cryptographic Security Measures.* The EUDI Wallet architecture implements multiple layers of cryptographic protection to secure both stored credentials and data exchanges. All personal data and attestations stored within the Wallet Instance must be encrypted at rest using strong encryption algorithms, preventing unauthorized access even if an attacker gains physical device access. Additionally, all data transmitted between the wallet and external entities—including PID Providers, Attestation Providers, and Relying Parties—must be encrypted in transit using protocols such as Transport Layer Security (TLS) with appropriate cipher suites. These measures ensure confidentiality and integrity throughout the data lifecycle.

The Wallet Secure Cryptographic Device serves as the root of trust for cryptographic operations, securely generating, storing, and managing private keys associated with the user's digital identity. Cryptographic secrets must never be exported outside the WSCD, which typically resides in hardware-isolated environments such as embedded Secure Elements, Trusted Execution Environments (TEE), or Hardware Security Modules (HSM). This isolation prevents malware or compromised operating system components from extracting sensitive key material. The architecture also supports external cryptographic devices, such as NFC-enabled national identity cards containing certified chips, which can provide additional security for high-assurance use cases.

Key management protocols ensure cryptographic keys are generated with sufficient entropy, stored securely throughout their lifecycle, and destroyed or revoked when no longer needed or when compromise is suspected. The ARF specifies that key rotation and ephemeral session keys should be employed where feasible to prevent long-term tracking of user transactions. Furthermore, the wallet must support Qualified Electronic Signatures (QES), which require integration with Qualified Trust Service Providers (QTSP) and Qualified Signature Creation Devices (QSCD) to ensure digitally signed documents carry the same legal weight as handwritten signatures across all Member States [1, 12].

*5.1.4 Authentication and Access Control.* User authentication to the EUDI Wallet must employ multi-factor authentication (MFA) mechanisms to prevent unauthorized access. Typically, this involves combining something the user knows (such as a PIN or password) with something the user has (the WSCD itself) and optionally something the user is (biometric authentication such as fingerprint or facial recognition). Biometric authentication, when used, must be processed locally on the device in secure hardware enclaves to prevent biometric data exposure to the operating system or transmission to external servers.

The ARF mandates that authentication mechanisms align with strong customer authentication requirements under the Payment Services Directive 2 (PSD2), which similarly requires multi-factor authentication for payment transactions. The concept of Strong User Authentication (SUA) introduced in eIDAS 2.0 is designed to be virtually identical to PSD2's Strong Customer Authentication (SCA), facilitating integration with existing financial services infrastructure. However, the wallet must balance security with usability, ensuring authentication flows do not impose excessive friction on users while maintaining robust protection against credential theft and session hijacking.

Access control within the wallet extends beyond user authentication to encompass fine-grained permissions for credential disclosure. Users must explicitly authorize each credential presentation to Relying Parties, with the wallet interface clearly displaying what information is being requested and for what purpose. The ARF requires that Wallet Instances alert users if a Relying Party requests additional data beyond what they have registered for, giving users the option to reject such transactions. This consent-based model ensures users maintain meaningful control over their personal data and can prevent unauthorized or excessive data collection.

## 5.2 Privacy Compliance

*5.2.1 GDPR Alignment and Legal Framework.* The EUDI Wallet is designed to operate in full compliance with the General Data Protection Regulation (EU 2016/679), which establishes comprehensive rules for processing personal data within the European Union. The eIDAS 2.0 Regulation explicitly requires that all personal data processing within the EUDI ecosystem be carried out in accordance with GDPR principles, particularly emphasizing privacy by design and privacy by default. Article 5a of eIDAS 2.0 introduces specific provisions for protecting personal data in digital identity wallets, mandating that personal data relating to wallet provision be kept logically separate from any other data held by wallet providers.

GDPR compliance begins with adherence to core data processing principles articulated in Article 5(1) GDPR. The principle of lawfulness, fairness, and transparency requires that users be fully informed about what personal data is collected, for what purposes, and with whom it is shared. The wallet must provide clear, accessible information about data processing activities through user-friendly interfaces. The principle of purpose limitation ensures personal data is collected for specified, explicit, and legitimate purposes and not further processed in ways incompatible with those purposes. The principle of data minimization—perhaps the most critical for digital identity systems—mandates that personal data shall be adequate, relevant, and limited to what is necessary in relation to processing purposes [7].

The EUDI Wallet implements GDPR requirements through both architectural measures and user-facing features. Recital 15 of the

EUDI Regulation emphasizes that citizens must be able to request, select, store, delete, and share identity data while enabling selective disclosure [7]. This user empowerment aligns with the GDPR principle of giving data subjects control over their personal information. Additionally, the wallet must support data subject rights under GDPR, including the right of access (Article 15), the right to rectification (Article 16), the right to erasure (Article 17), and the right to data portability (Article 20). The wallet dashboard serves as the primary mechanism for users to exercise these rights.

*5.2.2 Data Minimization and Selective Disclosure.* Data minimization is implemented as a fundamental architectural principle in the EUDI Wallet, operationalized through selective disclosure capabilities allowing users to share only specific attributes required for a given transaction. Recital 59 of the EUDI Regulation defines selective disclosure as the capability for the wallet to present only a subset of user attributes from Person Identification Data (PID) or Electronic Attestations of Attributes (EAA) [3, 9]. The ARF mandates that all PID and (Qualified) EAA attestations must support selective disclosure using privacy-preserving formats such as Selective Disclosure JSON Web Tokens (SD-JWT) or mobile security objects based on ISO/IEC 18013-5 [3].

Selective disclosure enables users to prove specific facts about themselves without revealing unnecessary personal information. For example, when purchasing age-restricted goods, a user can demonstrate they are over a certain age threshold without disclosing their exact date of birth, full name, address, or other identifying details [5, 10]. This capability significantly reduces privacy risks and limits potential for unauthorized profiling or tracking. The ARF provides concrete guidance on implementing age verification using the `age_over_NN` data elements defined in ISO/IEC 18013-5, which allow users to prove they meet age requirements for various thresholds (e.g., 16, 18, 21) without revealing their birthdate.

The technical implementation of selective disclosure relies on cryptographic protocols that bind disclosed attributes to the wallet's cryptographic credentials while selectively revealing only requested data. SD-JWT, specified by the Internet Engineering Task Force (IETF), achieves this by cryptographically hashing individual claims within a credential, allowing the wallet to construct presentations that include only the hashes of undisclosed claims and the plaintext values of disclosed ones. Relying Parties can verify that disclosed attributes are authentic and have not been tampered with, but they cannot access attributes the user has chosen not to reveal. This approach provides mathematical guarantees of data minimization while maintaining integrity and authenticity of presented credentials.

*5.2.3 Privacy-Enhancing Technologies.* Beyond selective disclosure, the EUDI ecosystem incorporates advanced privacy-enhancing technologies (PETs) to further protect user privacy. Zero-knowledge proofs (ZKPs) represent a particularly powerful technique allowing users to prove statements about their attributes without revealing underlying data. Recital 59 of the regulation specifically calls for privacy-preserving technologies like zero-knowledge proofs to enable validation of statements without revealing personal data [9]. For instance, a user could prove their bank account balance exceeds a certain threshold without disclosing the exact amount, or prove membership in a professional organization without revealing their identity.

Zero-knowledge proofs provide stronger privacy guarantees than selective disclosure alone by eliminating the need to reveal any attribute values whatsoever. Instead, ZKPs enable cryptographic verification of predicates (logical statements) about attributes. However, practical deployment of general-purpose ZKPs in the EUDI context faces challenges related to technical complexity, computational performance, and standardization. The ARF acknowledges these challenges and currently treats ZKPs as an evolving Discussion Topic, with ongoing work to develop practical specifications and implementations that balance privacy benefits with usability and efficiency constraints.

Article 5a(16) of eIDAS 2.0 requires that the wallet prevent attestation providers and relying parties from tracking user behavior and ensure unlinkability [2, 8]. Unlinkability means different transactions performed by the same user cannot be correlated by relying parties or other ecosystem actors, preventing construction of comprehensive user profiles across services. The architecture achieves unlinkability through several mechanisms: prohibiting data collection on wallet usage, generating transaction-specific ephemeral keys, employing pseudonyms that differ across relying parties, and ensuring credential presentations contain no persistent identifiers enabling cross-service tracking. These technical safeguards, combined with legal prohibitions on unauthorized profiling, create a privacy-preserving environment where users can interact with digital services without fear of ubiquitous surveillance.

*5.2.4 User Control and Transparency.* The EUDI Wallet embeds user control and transparency as foundational design principles, ensuring individuals retain authority over their digital identities at all times [2, 10]. Users must provide explicit consent before any credential presentation, with the wallet interface displaying exactly what information is being shared, with whom, and for what purpose [10]. This consent-based model aligns with GDPR requirements that personal data processing be based on the data subject's freely given, specific, informed, and unambiguous consent (Article 6(1)(a) GDPR).

Article 5a(4) of eIDAS 2.0 mandates that the wallet provide a common dashboard enabling users to view an up-to-date list of Relying Parties with which they have established connections and, where applicable, all data exchanged. The dashboard must support users in tracking all transactions executed through the wallet, including at minimum the time and date of each transaction, counterpart identification, personal data requested, and data shared. Furthermore, the dashboard must enable users to quickly request erasure of personal data by a Relying Party under Article 17 GDPR (the "right to be forgotten") and to easily report Relying Parties to competent national Data Protection Authorities where allegedly unlawful or suspicious data requests are received.

Transparency extends to governance of Relying Parties themselves. Relying Parties intending to use the EUDI Wallet must register in the Member State where they are established, specifying their intended use of the wallet including the exact data they will request and reasons for doing so. This registration information is made publicly available online in a user-friendly format, allowing users and the wallet itself to verify that data requests align with registered purposes. The Wallet Unit must alert users if a Relying Party requests data beyond what they registered for, providing users with the option to reject such transactions. This architecture prevents over-identification—scenarios where Relying Parties request full identity disclosure when only specific attribute verification is necessary—and gives users meaningful control over data sharing practices.

*5.2.5 Pseudonymity and Unlinkability.* The EUDI Wallet must support user-generated pseudonyms enabling interactions with Relying Parties without revealing real-world identities except when legally required. Pseudonymous authentication serves as the default option, with full identification reserved for scenarios where legal obligations such as Know Your Customer (KYC) requirements or border control necessitate identity disclosure. Users can create and manage multiple pseudonyms, and Relying Parties cannot reject pseudonym-based authentication unless rejection is required by law.

To prevent pseudonyms from becoming tracking mechanisms, the Wallet Unit must generate pseudonyms local to each Relying Party, ensuring different pseudonyms are used with different services. This prevents cross-RP correlation, whereby use of the same pseudonym with multiple Relying Parties could enable those parties to link transactions and construct user profiles. The requirement for pseudonym unlinkability extends to all ecosystem participants, including PID Providers and Attestation Providers, who are prohibited from learning how users employ their issued credentials across different contexts. Article 5a(5) of eIDAS 2.0 explicitly requires that the wallet not provide any information to trust service providers of electronic attestations about the use of those attestations.

Data Protection Impact Assessments (DPIAs) are mandatory for Relying Parties prior to processing wallet data where assessments indicate high privacy risks. Recital 17 of eIDAS 2.0 requires Relying Parties to perform DPIAs and consult competent Data Protection Authorities before engaging in data processing activities that could result in high risk to individuals' rights and freedoms. This requirement ensures privacy risks are systematically evaluated and mitigated before new use cases are deployed, and that independent oversight mechanisms can intervene when necessary to protect fundamental rights.

## 5.3 Interoperability Compliance

*5.3.1 Standards and Protocols.* Interoperability is achieved through adoption of internationally recognized standards and protocols ensuring different Wallet Solutions can communicate seamlessly with issuers, verifiers, and other wallets across Member States. The ARF mandates compliance with multiple standardization bodies, including the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), and the OpenID Foundation (OIDF) [1, 11]. This multi-standard approach balances the need for flexibility across diverse use cases with the requirement for consistent, verifiable interoperability.

For credential data models, the ARF requires support for both the W3C Verifiable Credentials Data Model 1.1 and ISO/IEC 18013-5:2021 formats. The W3C VC Data Model provides a flexible, extensible framework for representing credentials across a wide range of use cases, from government-issued identity documents to educational diplomas and professional licenses. ISO/IEC 18013-5, originally developed for mobile driving licenses (mDL), defines a mobile document (mdoc) format optimized for offline verification and proximity presentation scenarios, using Concise Binary Object Representation (CBOR) encoding for compact data structures.

The ARF specifies that PID attestations and qualified electronic attestations must be issued in accordance with both data models, with SD-JWT used for W3C-based encoding and ISO/IEC 18013-5 mdoc format for CBOR-based encoding. This dual-format requirement ensures credentials can be presented in contexts favoring either online remote verification (where JSON-based formats are common) or offline proximity scenarios (where CBOR offers efficiency and is already widely deployed in ISO-compliant documents). The ability to support both formats enhances interoperability with existing systems while enabling future innovation.

*5.3.2 Presentation and Issuance Protocols.* For credential presentation, the EUDI Wallet implements distinct protocols depending on the interaction model. Remote presentation flows, where the user interacts with a Relying Party over the internet, utilize the OpenID for Verifiable Presentations (OpenID4VP) protocol in combination with the W3C Digital Credentials API. OpenID4VP extends the OAuth 2.0 authorization framework to support presentation of verifiable credentials, enabling Relying Parties to request specific attributes through standardized authorization requests and receive cryptographic proofs of credential possession and attribute validity. The protocol defines mechanisms for trust negotiation and mutual authentication, ensuring both the wallet and the Relying Party can verify each other's legitimacy before exchanging sensitive information.

Proximity presentation flows, where the user is physically near the Relying Party (such as at a border checkpoint or retail point of sale), adhere to ISO/IEC 18013-5 standards. This specification defines how a secure communication channel is established using technologies such as NFC, Bluetooth Low Energy, or QR codes, and how presentation requests and responses are exchanged offline without requiring internet connectivity. The ability to operate offline is critical for scenarios where network access is unavailable or unreliable, and ISO/IEC 18013-5 has been widely tested and deployed in mobile driving license programs across multiple jurisdictions, providing a proven foundation for EUDI implementations.

Credential issuance follows the OpenID for Verifiable Credential Issuance (OpenID4VCI) protocol, which defines how PID Providers and Attestation Providers can securely issue credentials to Wallet Instances. OpenID4VCI supports both synchronous issuance, where credentials are delivered immediately upon request, and asynchronous issuance, where issuers perform background verification before credential delivery. The protocol includes mechanisms for requesting holder binding, ensuring issued credentials are cryptographically bound to the user's WSCD keys and cannot be transferred to other devices or users without detection.

*5.3.3 Trust Infrastructure and Cross-Border Recognition.* Trust in the EUDI ecosystem is anchored through a hierarchical trust infrastructure enabling verifiers to validate credentials issued by providers in other Member States without requiring bilateral trust agreements. For ISO/IEC 18013-5-based credentials, the trust model employs an X.509-based Public Key Infrastructure (PKI) where each PID Provider operates an independent root certificate. Trust registries, maintained at national and European levels, publish issuer metadata including certificate chains, public keys, and revocation information. Relying Parties query these registries to retrieve cryptographic material necessary to verify credential signatures and validate issuer authenticity [4, 11].

For W3C-based credentials using SD-JWT, trust frameworks based on OpenID Federation provide similar functionality through a distributed trust model. OpenID Federation allows entities such as PID Providers, Relying Parties, and Wallet Providers to establish trust relationships through cryptographic proofs and metadata exchanges, eliminating the need for pre-negotiated bilateral agreements. The federation model supports hierarchical trust chains where intermediate entities can vouch for leaf entities, enabling scalable trust propagation across the EU ecosystem. The ARF specifies that trust frameworks must support certificate revocation mechanisms, allowing issuers to invalidate compromised or expired credentials and ensuring verifiers can reliably check credential status.

Cross-border recognition is a fundamental legal and technical requirement of eIDAS 2.0. Under the regulation, credentials issued by one Member State must be recognized and legally valid in all other Member States, eliminating historical fragmentation where national eID schemes operated in isolation [11]. This mutual recognition is underpinned by both technical interoperability—through common data formats, protocols, and trust mechanisms—and legal obligations that prohibit Member States from refusing credentials solely because they are issued in another jurisdiction. The ARF defines common attestation rulebooks specifying the structure, semantics, and legal value of credential types, ensuring a driving license issued in Portugal is understood and accepted by verifiers in Finland using identical technical parameters.

*5.3.4 Attestation Rulebooks and Schema Catalogues.* To support diverse use cases across sectors, the ARF introduces the concept of attestation rulebooks and schema catalogues. An attestation rulebook defines the structure, attributes, and validation rules for a specific credential type, ensuring all issuers and verifiers interpret the credential consistently. For example, the PID Rulebook specifies mandatory and optional attributes for Person Identification Data, their data types, encoding formats (CBOR for ISO mdoc and JSON for SD-JWT), and namespace identifiers distinguishing EU-wide attributes from national extensions.

The European Commission maintains a publicly accessible catalogue of attestation rulebooks for Qualified Electronic Attestations of Attributes (QEAA) and Public Electronic Attestations of Attributes (PuB-EAA) used within the EUDI ecosystem. This catalogue may also include rulebooks for non-qualified EAA to provide guidance for private sector attestations. Registration in the catalogue is voluntary and does not create automatic acceptance or cross-border recognition, but it facilitates discovery and understanding of available credential types. By publishing standardized rulebooks, the ARF enables Attestation Providers to know exactly how to structure credentials for specific use cases, and Relying Parties to request and validate attributes with confidence they are correctly interpreting the data.

Schema catalogues similarly provide controlled vocabularies and attribute definitions promoting semantic interoperability. Rather than requiring each Member State or sector to independently define attribute names and data types, the catalogues establish common conventions reducing ambiguity and integration effort. For instance, attributes related to date of birth, address, and educational qualifications are defined with consistent identifiers, formats, and legal interpretations, ensuring automated systems can process credentials without manual mapping or translation. The ARF's modular architecture allows Member States to define national attributes within domestic namespaces while maintaining compatibility with the EU-wide core attribute set.

*5.3.5 Large-Scale Pilots and Continuous Testing.* The European Commission has launched Large-Scale Pilots (LSPs) to test specifications in real-world use cases and validate interoperability across diverse implementations. The POTENTIAL consortium, one of the most prominent pilots, involves 19 European Member States plus Ukraine and over 140 public and private partners. Within POTENTIAL, real use cases such as bank account opening, SIM card registration, mobile driving licenses, qualified electronic signatures, e-prescriptions, and digital government services are being tested to evaluate the wallet's interoperability, security, and user-friendliness under operational conditions.

Feedback from the LSPs directly informs the evolution of the ARF and reference implementation. The OpenID Foundation conducted a major interoperability demonstration in May 2025, where multiple implementers tested their OpenID4VP implementations against each other and against open-source conformance tests. Participants included the consortium developing the EUDI Wallet reference implementation (Scytáles and Netcompany-Intrasoft), as well as major technology vendors and service providers. Results of these interoperability events are shared with ISO/IEC working groups, informing development of standards like ISO/IEC 18013-7 for online presentation flows.

Continuous testing and iterative refinement are essential to achieving robust interoperability in a complex ecosystem with diverse national systems, varying legal frameworks, and evolving technological capabilities. The ARF is designed to be flexible and adaptable, with regular updates incorporating lessons learned from pilot deployments and changes in underlying standards. Version 2.6.0 of the ARF reflects substantial input from stakeholder consultations and technical validation, and further iterations are planned as implementing acts and certification schemes mature. This collaborative, evidence-based approach ensures the EUDI Wallet ecosystem can scale successfully from pilot projects to full deployment by the end of 2026, when Member States are required to offer wallet solutions to all citizens and businesses [1, 12].

## 5.4 Summary

The EUDI Wallet's compliance with security, privacy, and interoperability requirements establishes a robust foundation for trustworthy digital identity across the European Union. Security compliance, achieved through Level of Assurance High certification, Common Criteria evaluations, and rigorous cryptographic protections, ensures wallet implementations can withstand sophisticated attacks and safeguard sensitive user credentials. Privacy compliance, grounded in GDPR principles and operationalized through selective disclosure, zero-knowledge proofs, and user-centric dashboards, empowers individuals to control their personal data while minimizing unnecessary information sharing [2, 10]. Interoperability compliance, built on internationally recognized standards from W3C, ISO, IETF, and OIDF, enables seamless credential exchange across borders and sectors, fostering a unified European digital identity ecosystem.

These three pillars of compliance are not independent but deeply interdependent. Security mechanisms such as cryptographic attestations and certified hardware components provide the technical foundation for privacy-enhancing features like selective disclosure and unlinkability. Interoperability standards ensure security and privacy guarantees are consistently implemented across diverse Wallet Solutions and can be reliably verified by any compliant Relying Party. The harmonized legal framework of eIDAS 2.0, combined with implementing regulations and technical specifications in the ARF, creates a comprehensive governance structure balancing innovation with protection of fundamental rights.

The EUDI Wallet represents a landmark initiative in digital identity, demonstrating that it is possible to combine user sovereignty, cross-border interoperability, and regulatory compliance within a single, coherent architecture [6, 10]. By adhering to these compliance frameworks, the wallet aims to foster widespread adoption among citizens, businesses, and governments, ultimately realizing the vision of a secure, privacy-respecting, and universally accepted digital identity for all Europeans [1, 12].

## 6 Conclusion

The European Digital Identity Wallet represents a transformative step toward a unified, secure, and privacy-preserving digital identity infrastructure for the European Union. Through the eIDAS 2.0 Regulation and the Architecture and Reference Framework v2.6.0, Europe has established a comprehensive legal and technical foundation that synthesizes Self-Sovereign Identity principles with institutional trust mechanisms, creating a hybrid model uniquely suited to the continent's regulatory landscape and democratic values.

This report has examined the multifaceted dimensions of the EUDI Wallet ecosystem, revealing how architectural design, organizational governance, and compliance frameworks converge to enable user sovereignty while maintaining high assurance and legal enforceability. The Wallet Unit architecture, with its modular separation of concerns between user interfaces, cryptographic operations, and backend services, embodies the principle of security-by-design. The integration of privacy-enhancing technologies—including selective disclosure, zero-knowledge proofs, and unlinkability mechanisms—demonstrates that data minimization and user control can be implemented not merely as regulatory requirements but as fundamental technical capabilities.

The alignment with Self-Sovereign Identity principles, while adapting them to European regulatory realities, positions the EUDI Wallet as a pragmatic evolution of decentralized identity concepts. By anchoring trust through qualified trust service providers rather than distributed ledgers, and by ensuring credentials carry legally binding force under eIDAS 2.0, the framework provides assurance levels necessary for sensitive applications while preserving the user-centric benefits of SSI. This synthesis demonstrates that institutional accountability and individual sovereignty need not be mutually exclusive—they can be complementary components of a robust digital identity system.

The complex ecosystem of entities, roles, and responsibilities outlined in this report underscores the collaborative nature of the EUDI initiative. Success depends not only on technical specifications and cryptographic protocols but also on clear governance structures, consistent certification processes, and coordinated implementation across Member States. The establishment of Conformity Assessment Bodies, Supervisory Authorities, and trust registries creates accountability mechanisms ensuring that all participants—from Wallet Providers to Relying Parties—operate within established parameters and respect user rights.

Compliance with security, privacy, and interoperability standards represents perhaps the most significant achievement of the EUDI framework. By requiring Level of Assurance High certification, implementing GDPR-aligned privacy protections, and mandating adherence to internationally recognized standards (W3C, ISO, IETF, OpenID), the ARF ensures that the EUDI Wallet can meet the demanding requirements of cross-border, multi-sector deployment. The Large-Scale Pilots currently underway across Europe provide crucial real-world validation of these specifications, generating feedback that will refine implementations as the 2026 deployment deadline approaches.

Looking forward, several challenges and opportunities merit attention. The practical deployment of advanced privacy-enhancing technologies, particularly zero-knowledge proofs, remains an area of active research and development. Balancing cryptographic sophistication with computational efficiency and user experience will be critical for widespread adoption. The governance of attestation rulebooks and schema catalogues must evolve to accommodate emerging use cases while maintaining interoperability and legal clarity. The integration of the EUDI Wallet with existing national identity systems, sectoral regulations, and legacy infrastructure will require careful coordination and phased migration strategies.

Furthermore, the success of the EUDI Wallet ultimately depends on user acceptance and trust. Citizens must perceive the wallet as genuinely serving their interests—enhancing convenience, protecting privacy, and enabling seamless access to services—rather than as a surveillance tool or bureaucratic imposition. The transparency mechanisms embedded in the architecture, including transaction dashboards and consent management interfaces, will be crucial for building and maintaining this trust. Education initiatives explaining the wallet's capabilities, limitations, and privacy guarantees will be essential for informed adoption.

The EUDI Wallet initiative also carries implications beyond Europe's borders. As the first continental-scale implementation of a legally binding, privacy-preserving digital identity framework, it may serve as a reference model for other jurisdictions grappling with similar challenges. The open standards adopted by the ARF, the interoperability mechanisms established for cross-border recognition, and the balance achieved between innovation and regulation may inform global conversations about digital identity governance in the coming decade.

In conclusion, the European Digital Identity Wallet represents a bold and necessary response to the challenges of digital transformation in an interconnected world. By combining cutting-edge cryptographic techniques with robust legal frameworks, by empowering individuals while maintaining institutional accountability, and by fostering interoperability while respecting diversity, the EUDI initiative charts a path toward digital identity systems that honor both technological possibility and fundamental human rights. As implementation proceeds over the coming years, the lessons learned—technical, organizational, and societal—will shape not only Europe's digital future but potentially the global trajectory of identity management in the twenty-first century.

## Acknowledgments

The authors would like to acknowledge the European Commission and the Member State delegations to the eIDAS Cooperation Group for their continued development and refinement of the Architecture and Reference Framework. We extend our gratitude to the research communities working on Self-Sovereign Identity, verifiable credentials, and privacy-enhancing technologies, whose foundational work underpins the technical architecture analyzed in this report. Special thanks to the teams behind the Large-Scale Pilots, particularly the POTENTIAL consortium, whose real-world testing provides invaluable insights into the practical implementation of these specifications. We also acknowledge the contributions of standards organizations—W3C, ISO, IETF, OpenID Foundation, and ETSI—whose open standards enable the interoperability that is central to the EUDI vision. Finally, we recognize the importance of civil society organizations and privacy advocates whose scrutiny and feedback help ensure that the EUDI Wallet ecosystem respects fundamental rights and serves the interests of European citizens.

## References

[1] European Commission. 2024. European Digital Identity Wallet Architecture and Reference Framework. https://github.com/eu-digital-identity-wallet. Accessed: 2025-10-29.

[2] Digital Identity Wallet Project Consortium. 2025. EU Digital Identity Wallet Project: Guiding principles. https://digital-identity-wallet.eu/project/guiding-principles The project outlines user-centricity as a guiding principle, emphasising that citizens have full control over their attributes and data and must have transparency regarding what is shared and with whom.

[3] European Digital Identity Wallet Consortium. 2024. European Digital Identity Wallet Architecture and Reference Framework: Definitions section. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/ Defines selective disclosure as the capability for the EUDI Wallet to present only a subset of user attributes from person identification data or electronic attestations of attributes.

[4] Gabriel Leal da Rocha Ribeiro. 2023. SSI Technology in the Context of eIDAS 2.0. Master's thesis, University of Porto. https://repositorio-aberto.up.pt/bitstream/10216/156528/2/655820.pdf Explains that the core of the EUDI framework follows the SSI holder–issuer–verifier model; trusted attestation services and registries support verification.

[5] DocuSign. 2025. The European Digital Identity Wallet: Shaping Europe's digital future. https://www.docusign.com/blog/european-digital-identity-wallet-future Blog post describing how the EUDI Wallet uses selective disclosure to prove attributes such as age without revealing full personal data; highlights that selective disclosure reduces fraud and gives users control over what they share.

[6] Gataca. 2022. Why the European Digital Identity Wallet needs Self-Sovereign Identity principles. https://gataca.io/blog/the-european-digital-identity-wallet-architecture-reference-framework/ Blog post outlining that the ARF includes SSI principles and highlights that the EUDI Wallet gives users complete control over their data, allowing them to decide what information to share, with whom and when.

[7] European Digital Identity Cooperation Group. 2025. G – Zero Knowledge Proof, Discussion topics. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.4.0/discussion-topics/g-zero-knowledge-proof/ Recital 15 of the European Digital Identity Regulation emphasises that citizens must be able to request, select, store, delete and share identity data while enabling selective disclosure.

[8] European Digital Identity Cooperation Group. 2025. G – Zero Knowledge Proof, Discussion topics. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.4.0/discussion-topics/g-zero-knowledge-proof/ Article 5a(16) of the regulation requires that the wallet prevents attestation providers or relying parties from tracking user behaviour and ensures unlinkability.

[9] European Digital Identity Cooperation Group. 2025. G – Zero Knowledge Proof, Discussion topics. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.4.0/discussion-topics/g-zero-knowledge-proof/ Recital 59 defines selective disclosure and calls for privacy-preserving technologies like zero-knowledge proofs to enable validation of statements without revealing personal data.

[10] ISC2. 2025. Explaining the EUDI Wallet – Europe's digital identity revamp and what businesses must know about it. https://www.isc2.org/Insights/2025/04/Understanding-the-European-Digital-Identity-Wallet Article emphasising that the EUDI Wallet aims to ensure personal data sovereignty; credentials are stored in a decentralised wallet controlled by the user.

[11] Finextra Research. 2025. What makes the EUDI wallet self-sovereign? https://www.finextra.com/blogposting/24356/what-makes-the-eudi-wallet-self-sovereign Opinion piece explaining that eIDAS2/EUDI adopts core SSI components: a user-controlled wallet, verifiable credentials, selective disclosure, trust registries and cross-EU interoperability.

[12] European Union. 2024. Regulation (EU) 2024/1183 on electronic identification and trust services for electronic transactions (eIDAS 2.0). https://eur-lex.europa.eu/eli/reg/2024/1183/oj. Official Journal of the European Union.