

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 [19].

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 [10, 11].

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 [18].

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 [7, 9].

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 [18].

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 [19].

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, 19].

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 (QEAs)* with EU-wide legal effect [19].
- **Wallet Provider / Wallet Unit** — Certified provider and Wallet components (Wallet Instance, WSCA, WSCD, back-end) 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. **QEAs** are EAAs issued by QTSPs and enjoy the highest legal assurance under eIDAS 2.0 [19]. **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, 19].

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.

- 349 • **Wallet Secure Cryptographic Application (WSCA)** –
350 The logical component that mediates communication be-
351 tween the Wallet Instance and the WSCD. It handles cryp-
352 tographic operations such as key usage, digital signatures,
353 and proof-of-possession while enforcing security and pri-
354 vacy policies.
- 355 • **Wallet Provider Backend** – The remote service oper-
356 ated by a certified Wallet Provider. It manages registration,
357 credential lifecycle functions, and secure communication
358 with PID and (Q)EAA Providers. Importantly, it cannot ac-
359 cess personal data or private keys, aligning with GDPR and
360 *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* [19], 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* [19]. QTSPs are responsible for issuing and managing trust elements such as

qualified certificates, electronic signatures, seals, timestamps, and electronic attestations of attributes (QEAs). 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

465 privacy-by-design and GDPR compliance principles established
 466 under eIDAS 2.0 [19]. Together, these protocol requirements guarantee
 467 secure and interoperable data flows across all Member States,
 468 supporting both cross-border trust and user sovereignty in the
 469 European Digital Identity ecosystem.
 470

471 2.6 Summary

472 The *Architectural Analysis* of the European Digital Identity Wallet
 473 demonstrates how the *Architecture and Reference Framework (ARF)*
 474 integrates security, interoperability, and user empowerment into
 475 a cohesive ecosystem governed by *eIDAS 2.0*. Each architectural
 476 layer—from identity management and trust services to data ex-
 477 change protocols—contributes to a unified model of digital identity
 478 that is verifiable, privacy-preserving, and legally enforceable across
 479 all Member States.
 480

481 By combining open standards such as the W3C Verifiable Crea-
 482 dentials, ISO/IEC 18013-5, and OpenID4VCI/4VP protocols with
 483 qualified trust services under the *ETSI EN 319 4xx* standards, the
 484 ARF establishes a harmonised foundation for secure credential is-
 485 suance, authentication, and validation. This architecture embodies
 486 the convergence of *Self-Sovereign Identity (SSI)* principles with in-
 487 stitutional trust, ensuring that European citizens retain sovereignty
 488 over their personal data while benefiting from legally recognised
 489 and interoperable digital identities [1, 19].
 490

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.

496 3 Self-Sovereign Principles

497 Self-Sovereign Identity (SSI) represents a paradigm shift in digital
 498 identity management, placing individuals at the centre of control
 499 over their personal data. Unlike traditional centralised systems
 500 where identity providers hold and assert credentials on behalf of
 501 users, SSI enables individuals to maintain their own cryptograph-
 502 ically signed attestations and selectively reveal attributes when
 503 interacting with services. The European Digital Identity (EUDI)
 504 Wallet adapts these foundational SSI principles within a legally
 505 binding regulatory framework to meet the requirements of eIDAS
 506 2.0 (Regulation 2024/1183). This section examines how the EUDI
 507 Wallet implements core SSI concepts: user sovereignty, verifiable
 508 credentials, selective disclosure, and privacy-enhancing techniques.
 509 It also highlights the architectural and governance differences that
 510 distinguish the EUDI Wallet from decentralised SSI implemen-
 511 tations.
 512

514 3.1 User Control and Data Sovereignty

515 The principle of user sovereignty, whereby individuals control the
 516 storage, management, and disclosure of their identity data, distin-
 517 guishes SSI from traditional identity systems. In the EUDI ecosys-
 518 tem, credentials reside on the user’s device rather than in centralised
 519 registries, and explicit consent is required before any attribute is
 520 shared with a relying party [10, 11]. Citizens may request, select,
 521 store, delete, and share identity data at their discretion, and the
 522

wallet architecture prevents both issuers and verifiers from tracking
 523 user behaviour across transactions [11].
 524

Independent analyses confirm that the EUDI Wallet grants users
 525 complete control over their credentials, allowing them to decide
 526 what information to reveal, with whom, and when [9, 13]. This
 527 decentralised storage model ensures that personal data sovereignty
 528 remains with the holder rather than service providers. Under eIDAS
 529 2.0, every Member State must provide at least one EUDI Wallet
 530 solution enabling citizens to access public and private services using
 531 their own verifiable credentials [7]. These provisions institutionalise
 532 data sovereignty as a fundamental right within the European digital
 533 identity ecosystem.
 534

535 3.2 Verifiable Credentials and Trust 536 Frameworks

The SSI model operates on a three-party trust relationship: issuers
 537 create digitally signed credentials, holders store them in their wallets,
 538 and verifiers accept cryptographic proofs of credential pos-
 539 session. The EUDI Architecture and Reference Framework (ARF)
 540 adopts this structure through Person Identification Data (PID) and
 541 Electronic Attestations of Attributes (EAAs), which are issued by
 542 qualified trust service providers under eIDAS 2.0 [7]. These attesta-
 543 tions are cryptographically bound to the holder through device keys
 544 and can be independently verified without contacting the issuer.
 545

Trust in this ecosystem is anchored through trust registries that
 546 allow verifiers to retrieve issuer metadata and validate certificate status,
 547 thereby supporting cross-border credential recognition [7, 17]. Crucially,
 548 the ARF does not mandate distributed ledger technologies.
 549 Instead, it relies on qualified trust service providers and public-
 550 private governance arrangements to establish trust [18]. This ap-
 551 proach distinguishes the EUDI Wallet from many blockchain-based
 552 SSI systems while maintaining the core verification benefits of
 553 cryptographically signed credentials.
 554

555 3.3 Selective Disclosure and Privacy-Enhancing 556 Techniques

Data minimisation, the practice of disclosing only the attributes
 557 necessary for a given transaction, is a cornerstone of SSI privacy
 558 protection. The ARF explicitly defines selective disclosure as the
 559 capability for the wallet to present a subset of user attributes from
 560 PID or EAA attestations [5]. High-level requirements mandate that
 561 all PID and EAA credentials support selective disclosure through
 562 privacy-preserving formats such as selective-disclosure JSON Web
 563 Tokens (SD-JWT) or mobile security objects [6].
 564

In practice, when a verifier requests proof of a specific attribute,
 565 the wallet constructs a presentation containing only the requested
 566 data. For example, a merchant can verify that a customer is over
 567 18 years old without learning the customer’s name, date of birth,
 568 or address [8, 14]. This capability reduces both privacy risks and
 569 fraud exposure while maintaining regulatory compliance.
 570

The discussion on zero-knowledge proofs within the ARF em-
 571 phasises the importance of privacy-preserving technologies that
 572 enable validators to confirm statements without accessing underly-
 573 ing personal data [12]. Recital 59 of the regulation specifically calls
 574 for techniques like zero-knowledge proofs to validate claims while
 575 preserving privacy, and Article 5a mandates that wallets prevent
 576

correlation of presentations across different services [11, 12]. 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 [15]. User-centricity ensures that holders retain the authority to decide which credentials to present and may revoke consent at any time [3, 16]. 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 [17]. 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, 11]. Security by design integrates strong authentication mechanisms, including multi-factor authentication, secure hardware for cryptographic key storage, and rigorous protocols for credential protection [4, 15]. 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 [18]. 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) [18]. 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, 19]. 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 (Ecosystem) 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 mostly 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) colocar referencia, we have almost 20 different entities involved 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 rules 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 (QEAs) under eIDAS 2.0 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

697	on authentic government registers or administrative databases.	755
698	- Authentic Source (AS): Authoritative registry or database (e.g., population, tax, vehicle, education) holding verified identity or attribute data used by issuers.	756
699	• Relying and Verifying Parties	757
700	- Relying Party (RP): Public or private entity that requests, receives, and verifies credentials or attributes from Wallet Users to provide access or services.	758
701	- Access Certificate Authority (ACA): Authority that issues and manages digital certificates used for mutual authentication between Wallets, Providers, and Relying Parties.	759
702	• Trust and Conformity Infrastructure	760
703	- Registrar (REG): Entity responsible for managing registries, identifiers, and metadata for participants to ensure technical discoverability and resolution.	761
704	- Provider of Registration Certificates (PRC): Entity that issues registration certificates binding organizational or technical identities to registered participants in the EUDI ecosystem.	762
705	• Technical Certification and Evaluation	763
706	- Conformity Assessment Body (CAB): Independent, accredited organization that evaluates Wallets, Providers, and components for compliance with the ARF and applicable standards.	764
707	- Attestation Scheme Provider (ASP): Entity that defines evaluation and attestation schemes, assurance levels, and certification criteria for use by CABs and accreditation bodies.	765
708	• Supervisory and Accreditation Authorities	766
709	- Supervisory Body (SB): National authority overseeing Wallet Providers, PID Providers, and Attribute Providers to ensure regulatory compliance under eIDAS 2.0.	767
710	- National Accreditation Body (NAB): National authority accrediting CABs and ensuring the competence, impartiality, and consistency of conformity assessments.	768
711	- Trusted List Provider (TLP): Entity maintaining and publishing trusted lists of qualified and supervised services for discoverability and trust verification.	769
712	• European Governance	770
713	- 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.	771

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.

- **User Role:**

2025-11-02 14:08. Page 7 of 1-14.

544	- Manage and control personal digital identity credentials stored in the Wallet Unit.	755
545	- Provide consent for data sharing with Relying Parties.	756
546	- Authenticate to access services using the Wallet.	757
547	• Issuer Roles:	758
548	- Verify user identities and issue Person Identification Data (PID) credentials.	759
549	- Issue Electronic Attestations of Attributes (EAAs) based on verified data from authentic sources.	760
550	- Ensure compliance with ARF standards during issuance processes.	761
551	• Provider Roles:	762
552	- Develop, deploy, and maintain Wallet Units in accordance with ARF requirements.	763
553	- Implement strong authentication and security measures for Wallet access.	764
554	- Ensure interoperability with other ecosystem entities.	765
555	• Trust Roles:	766
556	- Manage trust registries and metadata for ecosystem participants.	767
557	- Issue and manage access certificates for mutual authentication.	768
558	- Facilitate cross-border trust verification among Member States.	769
559	• Governance Roles:	770
560	- Maintain the EUDI Toolbox and ARF to ensure policy coherence.	771
561	- Oversee ecosystem governance and compliance across Member States.	772
562	- Promote interoperability and standardization within the ecosystem.	773
563	• Supervisory Roles:	774
564	- Monitor compliance of Wallet Providers and Issuers with regulatory requirements.	775
565	- Accredit Conformity Assessment Bodies (CABs) for technical evaluations.	776
566	- Publish trusted lists of qualified services for discoverability and trust verification.	777

4.3 Responsibilities

Each entity has legally binding responsibilities under the eIDAS 2.0 proposal and ARF v2.6.0 to ensure the secure, interoperable, and privacy-preserving operation of the EUDI Wallet Ecosystem. Here we look at 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.

544	• User Responsibilities:	794
545	- Safeguard Wallet credentials and private keys.	795
546	- Provide accurate information during identity proofing.	796
547	- Manage consent for data sharing with Relying Parties.	797
548	• Issuer Responsibilities:	798
549	- Verify user identities before issuing credentials.	799
550	- Ensure credentials comply with ARF standards.	800
551	- Maintain secure issuance processes.	801

802

803

804

805

806

807

808

809

810

811

812

- **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 [19]. 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

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

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

947 *5.1.3 Cryptographic Security Measures.* The EUDI Wallet architecture
 948 implements multiple layers of cryptographic protection to secure both stored credentials and data exchanges. All personal
 949 data and attestations stored within the Wallet Instance must be
 950 encrypted at rest using strong encryption algorithms, preventing
 951 unauthorized access even if an attacker gains physical device access.
 952 Additionally, all data transmitted between the wallet and external
 953 entities—including PID Providers, Attestation Providers, and Relying
 954 Parties—must be encrypted in transit using protocols such as
 955 Transport Layer Security (TLS) with appropriate cipher suites.
 956 These measures ensure confidentiality and integrity throughout
 957 the data lifecycle.

958 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.

959 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, 19].

960 *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

987 combining something the user knows (such as a PIN or password)
 988 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.

989 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.

990 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

1018 *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.

1019 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 [10].

1020 The EUDI Wallet implements GDPR requirements through both architectural measures and user-facing features. Recital 15 of the

1045 EUDI Regulation emphasizes that citizens must be able to request,
 1046 select, store, delete, and share identity data while enabling selective
 1047 disclosure [10]. This user empowerment aligns with the GDPR
 1048 principle of giving data subjects control over their personal information.
 1049 Additionally, the wallet must support data subject rights under
 1050 GDPR, including the right of access (Article 15), the right to rectification
 1051 (Article 16), the right to erasure (Article 17), and the right to data portability
 1052 (Article 20). The wallet dashboard serves as the primary mechanism for users to exercise these rights.
 1053

1054
 1055 *5.2.2 Data Minimization and Selective Disclosure.* Data minimization
 1056 is implemented as a fundamental architectural principle in
 1057 the EUDI Wallet, operationalized through selective disclosure ca-
 1058 pabilities allowing users to share only specific attributes required
 1059 for a given transaction. Recital 59 of the EUDI Regulation defines
 1060 selective disclosure as the capability for the wallet to present only
 1061 a subset of user attributes from Person Identification Data (PID) or
 1062 Electronic Attestations of Attributes (EAA) [5, 12]. The ARF mandates
 1063 that all PID and (Qualified) EAA attestations must support
 1064 selective disclosure using privacy-preserving formats such as Se-
 1065 lective Disclosure JSON Web Tokens (SD-JWT) or mobile security
 1066 objects based on ISO/IEC 18013-5 [6].

1067 Selective disclosure enables users to prove specific facts about
 1068 themselves without revealing unnecessary personal information.
 1069 For example, when purchasing age-restricted goods, a user can
 1070 demonstrate they are over a certain age threshold without disclos-
 1071 ing their exact date of birth, full name, address, or other identifying
 1072 details [8, 14]. This capability significantly reduces privacy risks
 1073 and limits potential for unauthorized profiling or tracking. The
 1074 ARF provides concrete guidance on implementing age verification
 1075 using the `age_over_NN` data elements defined in ISO/IEC 18013-5,
 1076 which allow users to prove they meet age requirements for various
 1077 thresholds (e.g., 16, 18, 21) without revealing their birthdate.
 1078

1079 The technical implementation of selective disclosure relies on
 1080 cryptographic protocols that bind disclosed attributes to the wallet's
 1081 cryptographic credentials while selectively revealing only requested
 1082 data. SD-JWT, specified by the Internet Engineering Task Force
 1083 (IETF), achieves this by cryptographically hashing individual claims
 1084 within a credential, allowing the wallet to construct presentations
 1085 that include only the hashes of undisclosed claims and the plaintext
 1086 values of disclosed ones. Relying Parties can verify that disclosed
 1087 attributes are authentic and have not been tampered with, but they
 1088 cannot access attributes the user has chosen not to reveal. This
 1089 approach provides mathematical guarantees of data minimization
 1090 while maintaining integrity and authenticity of presented creden-
 1091 tials.

1092
 1093 *5.2.3 Privacy-Enhancing Technologies.* Beyond selective disclosure,
 1094 the EUDI ecosystem incorporates advanced privacy-enhancing tech-
 1095 nologies (PETs) to further protect user privacy. Zero-knowledge
 1096 proofs (ZKPs) represent a particularly powerful technique allowing
 1097 users to prove statements about their attributes without revealing
 1098 underlying data. Recital 59 of the regulation specifically calls for
 1099 privacy-preserving technologies like zero-knowledge proofs to en-
 1100 able validation of statements without revealing personal data [12].
 1101 For instance, a user could prove their bank account balance exceeds
 1102 a certain threshold without disclosing the exact amount, or prove

1103 membership in a professional organization without revealing their
 1104 identity.

1105 Zero-knowledge proofs provide stronger privacy guarantees
 1106 than selective disclosure alone by eliminating the need to reveal any
 1107 attribute values whatsoever. Instead, ZKPs enable cryptographic
 1108 verification of predicates (logical statements) about attributes. How-
 1109 ever, practical deployment of general-purpose ZKPs in the EUDI
 1110 context faces challenges related to technical complexity, computa-
 1111 tional performance, and standardization. The ARF acknowledges
 1112 these challenges and currently treats ZKPs as an evolving Discus-
 1113 sion Topic, with ongoing work to develop practical specifications
 1114 and implementations that balance privacy benefits with usability
 1115 and efficiency constraints.

1116 Article 5a(16) of eIDAS 2.0 requires that the wallet prevent at-
 1117 testation providers and relying parties from tracking user behavior
 1118 and ensure unlinkability [2, 11]. Unlinkability means different trans-
 1119 actions performed by the same user cannot be correlated by relying
 1120 parties or other ecosystem actors, preventing construction of com-
 1121 prehensive user profiles across services. The architecture achieves
 1122 unlinkability through several mechanisms: prohibiting data col-
 1123 lection on wallet usage, generating transaction-specific ephemeral
 1124 keys, employing pseudonyms that differ across relying parties, and
 1125 ensuring credential presentations contain no persistent identifiers
 1126 enabling cross-service tracking. These technical safeguards, com-
 1127 bined with legal prohibitions on unauthorized profiling, create a
 1128 privacy-preserving environment where users can interact with
 1129 digital services without fear of ubiquitous surveillance.

1130
 1131 *5.2.4 User Control and Transparency.* The EUDI Wallet embeds
 1132 user control and transparency as foundational design principles,
 1133 ensuring individuals retain authority over their digital identities
 1134 at all times [3, 15]. Users must provide explicit consent before
 1135 any credential presentation, with the wallet interface displaying
 1136 exactly what information is being shared, with whom, and for
 1137 what purpose [16]. This consent-based model aligns with GDPR
 1138 requirements that personal data processing be based on the data
 1139 subject's freely given, specific, informed, and unambiguous consent
 1140 (Article 6(1)(a) GDPR).

1141 Article 5a(4) of eIDAS 2.0 mandates that the wallet provide a com-
 1142 mon dashboard enabling users to view an up-to-date list of Relying
 1143 Parties with which they have established connections and, where
 1144 applicable, all data exchanged. The dashboard must support users
 1145 in tracking all transactions executed through the wallet, including
 1146 at minimum the time and date of each transaction, counterpart
 1147 identification, personal data requested, and data shared. Further-
 1148 more, the dashboard must enable users to quickly request erasure of
 1149 personal data by a Relying Party under Article 17 GDPR (the "right
 1150 to be forgotten") and to easily report Relying Parties to competent
 1151 national Data Protection Authorities where allegedly unlawful or
 1152 suspicious data requests are received.

1153 Transparency extends to governance of Relying Parties them-
 1154 selves. Relying Parties intending to use the EUDI Wallet must reg-
 1155 ister in the Member State where they are established, specifying
 1156 their intended use of the wallet including the exact data they will
 1157 request and reasons for doing so. This registration information is
 1158 made publicly available online in a user-friendly format, allowing
 1159 users and the wallet itself to verify that data requests align with

1161 registered purposes. The Wallet Unit must alert users if a Relying
 1162 Party requests data beyond what they registered for, providing users
 1163 with the option to reject such transactions. This architecture pre-
 1164 vents over-identification—scenarios where Relying Parties request
 1165 full identity disclosure when only specific attribute verification is
 1166 necessary—and gives users meaningful control over data sharing
 1167 practices.

1168
 1169 *5.2.5 Pseudonymity and Unlinkability.* The EUDI Wallet must sup-
 1170 port user-generated pseudonyms enabling interactions with Re-
 1171 lying Parties without revealing real-world identities except when
 1172 legally required. Pseudonymous authentication serves as the default
 1173 option, with full identification reserved for scenarios where legal
 1174 obligations such as Know Your Customer (KYC) requirements or
 1175 border control necessitate identity disclosure. Users can create and
 1176 manage multiple pseudonyms, and Relying Parties cannot reject
 1177 pseudonym-based authentication unless rejection is required by
 1178 law.

1179 To prevent pseudonyms from becoming tracking mechanisms,
 1180 the Wallet Unit must generate pseudonyms local to each Relying
 1181 Party, ensuring different pseudonyms are used with different ser-
 1182 vices. This prevents cross-RP correlation, whereby use of the same
 1183 pseudonym with multiple Relying Parties could enable those parties
 1184 to link transactions and construct user profiles. The requirement
 1185 for pseudonym unlinkability extends to all ecosystem participants,
 1186 including PID Providers and Attestation Providers, who are prohib-
 1187 ited from learning how users employ their issued credentials across
 1188 different contexts. Article 5a(5) of eIDAS 2.0 explicitly requires that
 1189 the wallet not provide any information to trust service providers
 1190 of electronic attestations about the use of those attestations.

1191 Data Protection Impact Assessments (DPIAs) are mandatory for
 1192 Relying Parties prior to processing wallet data where assessments
 1193 indicate high privacy risks. Recital 17 of eIDAS 2.0 requires Relying
 1194 Parties to perform DPIAs and consult competent Data Protection
 1195 Authorities before engaging in data processing activities that could
 1196 result in high risk to individuals' rights and freedoms. This re-
 1197 quirement ensures privacy risks are systematically evaluated and
 1198 mitigated before new use cases are deployed, and that independent
 1199 oversight mechanisms can intervene when necessary to protect
 1200 fundamental rights.

1201 **5.3 Interoperability Compliance**

1202
 1203 *5.3.1 Standards and Protocols.* Interoperability is achieved through
 1204 adoption of internationally recognized standards and protocols
 1205 ensuring different Wallet Solutions can communicate seamlessly
 1206 with issuers, verifiers, and other wallets across Member States. The
 1207 ARF mandates compliance with multiple standardization bodies,
 1208 including the World Wide Web Consortium (W3C), the Internet
 1209 Engineering Task Force (IETF), the International Organization for
 1210 Standardization (ISO), and the OpenID Foundation (OIDF) [1, 17].
 1211 This multi-standard approach balances the need for flexibility across
 1212 diverse use cases with the requirement for consistent, verifiable
 1213 interoperability.

1214 For credential data models, the ARF requires support for both
 1215 the W3C Verifiable Credentials Data Model 1.1 and ISO/IEC 18013-
 1216 5:2021 formats. The W3C VC Data Model provides a flexible, exten-
 1217 sible framework for representing credentials across a wide range

1219 of use cases, from government-issued identity documents to educa-
 1220 tional diplomas and professional licenses. ISO/IEC 18013-5, origi-
 1221 nally developed for mobile driving licenses (mDL), defines a mo-
 1222 bile document (mdoc) format optimized for offline verification and
 1223 proximity presentation scenarios, using Concise Binary Object Rep-
 1224 resentation (CBOR) encoding for compact data structures.

1225 The ARF specifies that PID attestations and qualified electronic
 1226 attestations must be issued in accordance with both data models,
 1227 with SD-JWT used for W3C-based encoding and ISO/IEC 18013-5
 1228 mdoc format for CBOR-based encoding. This dual-format require-
 1229 ment ensures credentials can be presented in contexts favoring
 1230 either online remote verification (where JSON-based formats are
 1231 common) or offline proximity scenarios (where CBOR offers effi-
 1232 ciency and is already widely deployed in ISO-compliant documents).
 1233 The ability to support both formats enhances interoperability with
 1234 existing systems while enabling future innovation.

1235
 1236 *5.3.2 Presentation and Issuance Protocols.* For credential presen-
 1237 tation, the EUDI Wallet implements distinct protocols depending
 1238 on the interaction model. Remote presentation flows, where the
 1239 user interacts with a Relying Party over the internet, utilize the
 1240 OpenID for Verifiable Presentations (OpenID4VP) protocol in com-
 1241 bination with the W3C Digital Credentials API. OpenID4VP extends
 1242 the OAuth 2.0 authorization framework to support presentation
 1243 of verifiable credentials, enabling Relying Parties to request spe-
 1244 cific attributes through standardized authorization requests and
 1245 receive cryptographic proofs of credential possession and attribute
 1246 validity. The protocol defines mechanisms for trust negotiation and
 1247 mutual authentication, ensuring both the wallet and the Relying
 1248 Party can verify each other's legitimacy before exchanging sensitive
 1249 information.

1250 Proximity presentation flows, where the user is physically near
 1251 the Relying Party (such as at a border checkpoint or retail point
 1252 of sale), adhere to ISO/IEC 18013-5 standards. This specification
 1253 defines how a secure communication channel is established using
 1254 technologies such as NFC, Bluetooth Low Energy, or QR codes,
 1255 and how presentation requests and responses are exchanged off-
 1256 line without requiring internet connectivity. The ability to operate
 1257 offline is critical for scenarios where network access is unavail-
 1258 able or unreliable, and ISO/IEC 18013-5 has been widely tested and
 1259 deployed in mobile driving license programs across multiple juris-
 1260 dictions, providing a proven foundation for EUDI implementations.

1261 Credential issuance follows the OpenID for Verifiable Credential
 1262 Issuance (OpenID4VCI) protocol, which defines how PID Providers
 1263 and Attestation Providers can securely issue credentials to Wal-
 1264 let Instances. OpenID4VCI supports both synchronous issuance,
 1265 where credentials are delivered immediately upon request, and
 1266 asynchronous issuance, where issuers perform background veri-
 1267 fication before credential delivery. The protocol includes mecha-
 1268 nisms for requesting holder binding, ensuring issued credentials
 1269 are cryptographically bound to the user's WSCD keys and cannot
 1270 be transferred to other devices or users without detection.

1271
 1272 *5.3.3 Trust Infrastructure and Cross-Border Recognition.* Trust in
 1273 the EUDI ecosystem is anchored through a hierarchical trust in-
 1274 frastructure enabling verifiers to validate credentials issued by
 1275 providers in other Member States without requiring bilateral trust
 1276 agreements. For ISO/IEC 18013-5-based credentials, the trust model

1277 employs an X.509-based Public Key Infrastructure (PKI) where each
 1278 PID Provider operates an independent root certificate. Trust registries,
 1279 maintained at national and European levels, publish issuer metadata
 1280 including certificate chains, public keys, and revocation information.
 1281 Relying Parties query these registries to retrieve cryptographic material
 1282 necessary to verify credential signatures and validate issuer authenticity [7, 17].
 1283

1284 For W3C-based credentials using SD-JWT, trust frameworks
 1285 based on OpenID Federation provide similar functionality through
 1286 a distributed trust model. OpenID Federation allows entities such
 1287 as PID Providers, Relying Parties, and Wallet Providers to establish
 1288 trust relationships through cryptographic proofs and metadata
 1289 exchanges, eliminating the need for pre-negotiated bilateral agreements.
 1290 The federation model supports hierarchical trust chains
 1291 where intermediate entities can vouch for leaf entities, enabling
 1292 scalable trust propagation across the EU ecosystem. The ARF specifies
 1293 that trust frameworks must support certificate revocation mechanisms,
 1294 allowing issuers to invalidate compromised or expired credentials
 1295 and ensuring verifiers can reliably check credential status.

1296 Cross-border recognition is a fundamental legal and technical
 1297 requirement of eIDAS 2.0. Under the regulation, credentials issued
 1298 by one Member State must be recognized and legally valid in all
 1299 other Member States, eliminating historical fragmentation where
 1300 national eID schemes operated in isolation [18]. This mutual recogni-
 1301 tion is underpinned by both technical interoperability—through
 1302 common data formats, protocols, and trust mechanisms—and legal
 1303 obligations that prohibit Member States from refusing credentials
 1304 solely because they are issued in another jurisdiction. The ARF
 1305 defines common attestation rulebooks specifying the structure, se-
 1306 mantics, and legal value of credential types, ensuring a driving
 1307 license issued in Portugal is understood and accepted by verifiers
 1308 in Finland using identical technical parameters.

1309
 1310
 1311 *5.3.4 Attestation Rulebooks and Schema Catalogues.* To support
 1312 diverse use cases across sectors, the ARF introduces the concept
 1313 of attestation rulebooks and schema catalogues. An attestation
 1314 rulebook defines the structure, attributes, and validation rules for a
 1315 specific credential type, ensuring all issuers and verifiers interpret
 1316 the credential consistently. For example, the PID Rulebook specifies
 1317 mandatory and optional attributes for Person Identification Data,
 1318 their data types, encoding formats (CBOR for ISO mdm and JSON
 1319 for SD-JWT), and namespace identifiers distinguishing EU-wide
 1320 attributes from national extensions.

1321 The European Commission maintains a publicly accessible cat-
 1322 alogue of attestation rulebooks for Qualified Electronic Attestations
 1323 of Attributes (QEAA) and Public Electronic Attestations of
 1324 Attributes (PuB-EAA) used within the EUDI ecosystem. This cata-
 1325 logue may also include rulebooks for non-qualified EAA to provide
 1326 guidance for private sector attestations. Registration in the cata-
 1327 logue is voluntary and does not create automatic acceptance or
 1328 cross-border recognition, but it facilitates discovery and under-
 1329 standing of available credential types. By publishing standardized
 1330 rulebooks, the ARF enables Attestation Providers to know exactly
 1331 how to structure credentials for specific use cases, and Relying
 1332 Parties to request and validate attributes with confidence they are
 1333 correctly interpreting the data.

1334 Schema catalogues similarly provide controlled vocabularies and
 1335 attribute definitions promoting semantic interoperability. Rather
 1336 than requiring each Member State or sector to independently define
 1337 attribute names and data types, the catalogues establish common
 1338 conventions reducing ambiguity and integration effort. For instance,
 1339 attributes related to date of birth, address, and educational qualifi-
 1340 cations are defined with consistent identifiers, formats, and legal
 1341 interpretations, ensuring automated systems can process creden-
 1342 tials without manual mapping or translation. The ARF’s modular
 1343 architecture allows Member States to define national attributes
 1344 within domestic namespaces while maintaining compatibility with
 1345 the EU-wide core attribute set.

1346
 1347 *5.3.5 Large-Scale Pilots and Continuous Testing.* The European
 1348 Commission has launched Large-Scale Pilots (LSPs) to test specifi-
 1349 cations in real-world use cases and validate interoperability across
 1350 diverse implementations. The POTENTIAL consortium, one of the
 1351 most prominent pilots, involves 19 European Member States plus
 1352 Ukraine and over 140 public and private partners. Within POTEN-
 1353 TIAL, real use cases such as bank account opening, SIM card regis-
 1354 tration, mobile driving licenses, qualified electronic signatures,
 1355 e-prescriptions, and digital government services are being tested to
 1356 evaluate the wallet’s interoperability, security, and user-friendliness
 1357 under operational conditions.

1358 Feedback from the LSPs directly informs the evolution of the ARF
 1359 and reference implementation. The OpenID Foundation conducted a
 1360 major interoperability demonstration in May 2025, where multiple
 1361 implementers tested their OpenID4VP implementations against
 1362 each other and against open-source conformance tests. Participants
 1363 included the consortium developing the EUDI Wallet reference
 1364 implementation (Scytlés and Netcompany-Intrasoft), as well as
 1365 major technology vendors and service providers. Results of these
 1366 interoperability events are shared with ISO/IEC working groups,
 1367 informing development of standards like ISO/IEC 18013-7 for online
 1368 presentation flows.

1369 Continuous testing and iterative refinement are essential to
 1370 achieving robust interoperability in a complex ecosystem with
 1371 diverse national systems, varying legal frameworks, and evolving
 1372 technological capabilities. The ARF is designed to be flexible and
 1373 adaptable, with regular updates incorporating lessons learned from
 1374 pilot deployments and changes in underlying standards. Version
 1375 2.6.0 of the ARF reflects substantial input from stakeholder consulta-
 1376 tions and technical validation, and further iterations are planned as
 1377 implementing acts and certification schemes mature. This collabora-
 1378 tive, evidence-based approach ensures the EUDI Wallet ecosystem
 1379 can scale successfully from pilot projects to full deployment by
 1380 the end of 2026, when Member States are required to offer wallet
 1381 solutions to all citizens and businesses [1, 19].

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

1382
 1383
 1384
 1385
 1386
 1387
 1388
 1389
 1390
 1391
 1392

1393 attacks and safeguard sensitive user credentials. Privacy compli-
 1394 ance, grounded in GDPR principles and operationalized through
 1395 selective disclosure, zero-knowledge proofs, and user-centric dash-
 1396 boards, empowers individuals to control their personal data while
 1397 minimizing unnecessary information sharing [2, 4, 15]. Interopera-
 1398 bility compliance, built on internationally recognized standards
 1399 from W3C, ISO, IETF, and OIDF, enables seamless credential ex-
 1400 change across borders and sectors, fostering a unified European
 1401 digital identity ecosystem.

1402 These three pillars of compliance are not independent but deeply
 1403 interdependent. Security mechanisms such as cryptographic attes-
 1404 tations and certified hardware components provide the technical
 1405 foundation for privacy-enhancing features like selective disclosure
 1406 and unlinkability. Interoperability standards ensure security and
 1407 privacy guarantees are consistently implemented across diverse
 1408 Wallet Solutions and can be reliably verified by any compliant Rely-
 1409 ing Party. The harmonized legal framework of eIDAS 2.0, combined
 1410 with implementing regulations and technical specifications in the
 1411 ARF, creates a comprehensive governance structure balancing in-
 1412 novation with protection of fundamental rights.

1413 The EUDI Wallet represents a landmark initiative in digital iden-
 1414 tity, demonstrating that it is possible to combine user sovereignty,
 1415 cross-border interoperability, and regulatory compliance within a
 1416 single, coherent architecture [9, 13]. By adhering to these compli-
 1417 ance frameworks, the wallet aims to foster widespread adoption
 1418 among citizens, businesses, and governments, ultimately realizing
 1419 the vision of a secure, privacy-respecting, and universally accepted
 1420 digital identity for all Europeans [1, 19].

1422 6 Conclusion

1423 The European Digital Identity Wallet represents a transformative
 1424 step toward a unified, secure, and privacy-preserving digital iden-
 1425 tity infrastructure for the European Union. Through the eIDAS 2.0
 1426 Regulation and the Architecture and Reference Framework v2.6.0,
 1427 Europe has established a comprehensive legal and technical founda-
 1428 tion that synthesizes Self-Sovereign Identity principles with insti-
 1429 tutional trust mechanisms, creating a hybrid model uniquely suited
 1430 to the continent's regulatory landscape and democratic values.

1431 This report has examined the multifaceted dimensions of the
 1432 EUDI Wallet ecosystem, revealing how architectural design, or-
 1433 ganizational governance, and compliance frameworks converge
 1434 to enable user sovereignty while maintaining high assurance and
 1435 legal enforceability. The Wallet Unit architecture, with its modular
 1436 separation of concerns between user interfaces, cryptographic op-
 1437 erations, and backend services, embodies the principle of security-by-
 1438 design. The integration of privacy-enhancing technologies—including
 1439 selective disclosure, zero-knowledge proofs, and unlinkability mech-
 1440 anisms—demonstrates that data minimization and user control can
 1441 be implemented not merely as regulatory requirements but as fun-
 1442 damental technical capabilities.

1443 The alignment with Self-Sovereign Identity principles, while
 1444 adapting them to European regulatory realities, positions the EUDI
 1445 Wallet as a pragmatic evolution of decentralized identity concepts.
 1446 By anchoring trust through qualified trust service providers rather
 1447 than distributed ledgers, and by ensuring credentials carry legally
 1448 binding force under eIDAS 2.0, the framework provides assurance

1449 levels necessary for sensitive applications while preserving the
 1450 user-centric benefits of SSI. This synthesis demonstrates that in-
 1451 stitutional accountability and individual sovereignty need not be
 1452 mutually exclusive—they can be complementary components of a
 1453 robust digital identity system.

1454 The complex ecosystem of entities, roles, and responsibilities out-
 1455 lined in this report underscores the collaborative nature of the EUDI
 1456 initiative. Success depends not only on technical specifications and
 1457 cryptographic protocols but also on clear governance structures,
 1458 consistent certification processes, and coordinated implementation
 1459 across Member States. The establishment of Conformity Assess-
 1460 ment Bodies, Supervisory Authorities, and trust registries creates
 1461 accountability mechanisms ensuring that all participants—from
 1462 Wallet Providers to Relying Parties—operate within established
 1463 parameters and respect user rights.

1464 Compliance with security, privacy, and interoperability stan-
 1465 dards represents perhaps the most significant achievement of the
 1466 EUDI framework. By requiring Level of Assurance High certifica-
 1467 tion, implementing GDPR-aligned privacy protections, and mandat-
 1468 ing adherence to internationally recognized standards (W3C, ISO,
 1469 IETF, OpenID), the ARF ensures that the EUDI Wallet can meet the
 1470 demanding requirements of cross-border, multi-sector deployment.
 1471 The Large-Scale Pilots currently underway across Europe provide
 1472 crucial real-world validation of these specifications, generating
 1473 feedback that will refine implementations as the 2026 deployment
 1474 deadline approaches.

1475 Looking forward, several challenges and opportunities merit at-
 1476 tention. The practical deployment of advanced privacy-enhancing
 1477 technologies, particularly zero-knowledge proofs, remains an area
 1478 of active research and development. Balancing cryptographic so-
 1479 phistication with computational efficiency and user experience will
 1480 be critical for widespread adoption. The governance of attestation
 1481 rulebooks and schema catalogues must evolve to accommodate
 1482 emerging use cases while maintaining interoperability and legal
 1483 clarity. The integration of the EUDI Wallet with existing national
 1484 identity systems, sectoral regulations, and legacy infrastructure
 1485 will require careful coordination and phased migration strategies.

1486 Furthermore, the success of the EUDI Wallet ultimately depends
 1487 on user acceptance and trust. Citizens must perceive the wallet as
 1488 genuinely serving their interests—enhancing convenience, protect-
 1489 ing privacy, and enabling seamless access to services—rather than
 1490 as a surveillance tool or bureaucratic imposition. The transparency
 1491 mechanisms embedded in the architecture, including transaction
 1492 dashboards and consent management interfaces, will be crucial for
 1493 building and maintaining this trust. Education initiatives explaining
 1494 the wallet's capabilities, limitations, and privacy guarantees will be
 1495 essential for informed adoption.

1496 The EUDI Wallet initiative also carries implications beyond Eu-
 1497 rope's borders. As the first continental-scale implementation of a
 1498 legally binding, privacy-preserving digital identity framework, it
 1499 may serve as a reference model for other jurisdictions grappling
 1500 with similar challenges. The open standards adopted by the ARF,
 1501 the interoperability mechanisms established for cross-border recog-
 1502 nition, and the balance achieved between innovation and regulation
 1503 may inform global conversations about digital identity governance
 1504 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> Describes the privacy-by-design principle: data minimisation and enabling selective disclosure, using zero-knowledge proofs and robust safeguards to prevent tracking or linkability of the holder.
- [3] 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.
- [4] Digital Identity Wallet Project Consortium. 2025. EU Digital Identity Wallet Project: Guiding principles. <https://digital-identity-wallet.eu/project/guiding-principles> Highlights security-by-design: integrating strong security mechanisms from the outset to protect identity data stored and transmitted through the wallet.
- [5] 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.
- [6] European Digital Identity Wallet Consortium. 2024. European Digital Identity Wallet Architecture and Reference Framework: Requirements for attestation issuance. <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/> Mandates that Person Identification Data and (Qualified) Electronic Attestations of Attributes must support selective disclosure using SD-JWT or mobile security objects.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] 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> The article provides an example where a merchant can verify a customer is over 18 without seeing their full identity, demonstrating selective disclosure capabilities.
- [15] 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> Lists the guiding principles for the EUDI Wallet: user-centricity, interoperability, privacy by design and security by design.
- [16] 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> Describes how the wallet requires user consent before any attribute is shared and that users can use selective disclosure or zero-knowledge proofs to share only necessary attributes.
- [17] 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.
- [18] Finextra Research. 2025. What makes the EUDI wallet self-sovereign? <https://www.finextra.com/blogposting/24356/what-makes-the-eudi-wallet-self-sovereign> The article contrasts the EUDI wallet with classic SSI approaches, noting that it does not mandate a blockchain, provides legally binding signatures and operates under a public–private governance framework.
- [19] 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.

1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624