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 focuses on a component-level evaluation of the ARF and on the conceptual design of a pilot implementation, analysing how identity verification, privacy safeguards, and interoperability mechanisms support concrete digital identity transactions in practice.

Keywords

European Digital Identity Wallet, eIDAS 2.0, Architecture and Reference Framework, Digital Identity, Interoperability, Privacy-by-Design

1 Introduction

The goal of this project is to investigate which specific components of the European Digital Identity Wallet cro:ARFArchitecture and Reference Framework (ARF) effectively support digital identity transactions under the eIDAS 2.0 framework. Rather than providing another broad, descriptive overview of the ecosystem, this work narrows its focus to two complementary tasks:

- a *component evaluation* of key architectural building blocks that enable secure identification, privacy-preserving attribute exchange, and cross-border interoperability; and
- a *pilot design* that illustrates, at a high level, how those components can be orchestrated in a concrete use case.

In particular, we analyse: (i) how identity verification and authentication are realised across different Levels of Assurance (cro:LoALevel of Assurance (LoA)), (ii) how data minimisation and consent management mechanisms contribute to cro:GDPRGeneral Data Protection Regulation (GDPR) compliance, and (iii) which interoperability mechanisms allow national identity systems and sectoral services to interact smoothly while sharing a common architectural baseline.

Building on this analysis, we then propose a minimally functional pilot design for a specific use case, describing the actors involved, the flow of credentials and trust, and the way architectural principles from the ARF are applied in practice.

1.1 Structure of the Report

The remainder of this report is structured as follows. Section 2 presents the component evaluation, organised around identity verification and authentication, privacy safeguards, and interoperability mechanisms. Section **??** introduces a high-level pilot design for a chosen use case, mapping the components analysed in Section 2 to a practical flow of identity and trust. Section 4 concludes the report with a short reflection on the strengths and limitations of the ARF in supporting real-world deployments.

2 Component Evaluation

The ARF defines a set of technical and organisational components that work together to support digital identity transactions, from initial identity proofing to the presentation of attributes to Relying Parties. In this section, we evaluate those components along three dimensions explicitly required by the assignment: identity verification and authentication, data minimisation and consent management, and interoperability mechanisms.

2.1 Identity Verification and Authentication

2.1.1 Identity Proofing and PID Issuance.

2.1.2 Authentication of the Holder.

2.1.3 Mutual Authentication with Relying Parties.

2.2 Data Minimisation and Consent Management

Data minimisation, a cornerstone principle of the General Data Protection Regulation (GDPR), requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The ARF operationalises this principle through selective disclosure mechanisms, explicit consent flows, and architectural safeguards that prevent unauthorised tracking and correlation of user activities across services. These technical and organisational measures ensure that the EUDI Wallet not only complies with legal obligations but embeds privacy protection as a fundamental design characteristic.

2.2.1 Selective Disclosure of Attributes. Selective disclosure enables users to present only the specific attributes required for a given transaction, withholding all other personal information even when it resides within the same credential. The ARF mandates that all Person Identification Data (PID) and Electronic Attestation of Attributes (EAA) credentials support selective disclosure using privacy-preserving formats [8]. Two primary technical mechanisms implement this capability: Selective Disclosure JSON Web Tokens (SD-JWT) for credentials based on the W3C Verifiable Credentials

Data Model, and the mobile document (mdoc) format defined in ISO/IEC 18013-5:2021 for CBOR-encoded credentials.

SD-JWT achieves selective disclosure by cryptographically hashing individual claims within a credential separately, allowing the wallet to construct presentations that include only the plaintext values of disclosed attributes alongside the hashes of undisclosed ones. When a Relying Party requests proof of a specific attribute, for example, confirmation that a user is over 18 years of age, the wallet can reveal only the `age_over_18` boolean claim without disclosing the user's exact date of birth, full name, address, or any other personal identifiers contained in the PID [10, 16]. The Relying Party can cryptographically verify that the disclosed attribute is authentic and has not been tampered with, but cannot access any information the user has chosen to withhold.

Similarly, the ISO/IEC 18013-5 mdoc format structures credentials as a collection of data elements within defined namespaces, enabling fine-grained disclosure control. During proximity presentations using NFC or Bluetooth, the wallet presents only the requested data elements while maintaining cryptographic binding to the issuer's signature. This approach is particularly effective for offline verification scenarios where network connectivity is unavailable, such as age verification at retail points of sale or document checks at border crossings.

The ARF further defines specific mechanisms for age verification without date of birth disclosure, leveraging the `age_over_NN` attributes specified in ISO/IEC 18013-5. These derived attributes allow users to prove they meet various age thresholds (e.g., 16, 18, 21) without revealing their precise birthdate, thereby minimising the personal data shared in common identity verification scenarios. This capability directly implements the data minimisation obligation under Article 5(1)(c) GDPR while maintaining the assurance level necessary for regulated activities [13, 14].

2.2.2 User Consent and Transparency. The principle of user control over personal data, central to both GDPR and Self-Sovereign Identity paradigms, is embedded throughout the wallet's consent and transparency mechanisms. Article 5a(4) of eIDAS 2.0 mandates that the wallet provide a common dashboard enabling users to view an up-to-date list of Relying Parties with which they have shared data, along with details of all exchanged information [19]. This dashboard must display, at minimum, the time and date of each transaction, the identity of the counterpart, the personal data requested, and the data actually shared.

Before any credential presentation, the wallet interface must present the user with clear, unambiguous information about what attributes are being requested, by whom, and for what stated purpose [7, 16]. Users must provide explicit consent for each disclosure, with the wallet ensuring that consent is freely given, specific, informed, and unambiguous as required by Article 4(11) and Article 7 GDPR. The ARF specifies that wallets must alert users if a Relying Party requests data beyond what it has registered for in the national registry, providing users the option to reject such transactions.

Relying Parties must register their intended uses of the EUDI Wallet with competent authorities in their Member State of establishment, specifying exactly which attributes they will request and the legal or contractual basis for doing so. This registration information is made publicly available online in user-friendly formats, allowing both users and the wallet itself to verify that data requests align with declared purposes. The registration requirement implements accountability obligations under Article 5(2) GDPR and provides transparency about data processing practices before users engage with services [5].

The dashboard also enables users to exercise their rights under GDPR, including the right to request erasure of personal data (Article 17) and the right to report suspected unlawful data processing to competent Data Protection Authorities. By consolidating transaction history, consent records, and data subject rights mechanisms in a single, accessible interface, the wallet operationalises the transparency obligations that underpin trust in personal data processing [7].

2.2.3 Unlinkability and Anti-Tracking Measures. Beyond selective disclosure and consent management, the ARF implements architectural measures to prevent tracking and correlation of user activities across different Relying Parties. Article 5a(16) of eIDAS 2.0 explicitly requires that the wallet prevent attestation providers or Relying Parties from tracking user behaviour and ensure unlinkability [15]. Unlinkability means that different transactions performed by the same user cannot be correlated by service providers, thereby preventing the construction of comprehensive user profiles without explicit consent.

The wallet achieves unlinkability through several technical mechanisms. First, credential presentations must not contain persistent identifiers that remain constant across different Relying Parties. Instead, the wallet generates transaction-specific or Relying Party-specific pseudonyms, ensuring that the same user appears with different identifiers to different services. Second, the wallet employs cryptographic proof-of-possession mechanisms that demonstrate control over credentials without revealing long-term private keys, preventing key-based tracking across presentations.

Third, the ARF mandates that PID Providers and Attestation Providers must not learn how users employ issued credentials. Article 5a(5) of eIDAS 2.0 prohibits wallets from providing any information to trust service providers about the use of attestations [19]. This "issuer blindness" prevents even trusted authorities from monitoring citizen interactions with private or public services, reinforcing privacy against surveillance by state actors and institutional service providers alike.

However, achieving perfect unlinkability while maintaining high assurance levels presents practical challenges. Certain high-risk transactions, such as financial services subject to anti-money laundering regulations, border control, or law enforcement investigations, may require linkable identifiers under legal obligations. The ARF acknowledges these tensions and provides mechanisms for pseudonymous authentication as the default mode, with full identification reserved for scenarios where legal mandates necessitate it. Users can create and manage multiple pseudonyms, and Relying Parties cannot reject pseudonym-based authentication unless required by law [5].

Moreover, practical implementation of unlinkability depends on broader ecosystem design beyond the wallet itself. If Relying Parties collude to correlate transactions based on timing, disclosed

attributes, or network metadata, architectural unlinkability guarantees may be circumvented. The regulatory framework addresses this through Data Protection Impact Assessments (DPIAs) required under Recital 17 of eIDAS 2.0, mandating that Relying Parties assess and mitigate high privacy risks before processing wallet data [19]. Supervisory authorities must be consulted where DPIAs indicate residual high risks, providing an institutional safeguard complementing technical privacy measures.

2.3 Interoperability Mechanisms

Interoperability, the ability for diverse systems implemented by different Member States, sectors, and providers to exchange and mutually recognise digital credentials, is fundamental to realising the EUDI Wallet's vision of a seamless European digital identity ecosystem. The ARF achieves interoperability through adherence to internationally recognised standards for credential formats, protocols for issuance and presentation, and a trust infrastructure that enables cross-border verification without requiring bilateral agreements between all parties. This section evaluates these mechanisms and their role in supporting the wallet's operational requirements.

2.3.1 Cross-Border Credential Formats. The ARF mandates support for two complementary credential data models: the W3C Verifiable Credentials Data Model 1.1 and the ISO/IEC 18013-5:2021 mobile document (mdoc) format [5]. This dual-format approach balances flexibility for diverse use cases with proven interoperability in high-assurance, offline scenarios. The W3C Verifiable Credentials Data Model provides an extensible JSON-based framework suitable for representing a wide range of attestations, from government-issued identity documents to educational diplomas, professional licenses, and sectoral credentials. Its flexibility enables innovation and adaptation to emerging use cases while maintaining a consistent verification model based on cryptographic signatures and decentralised identifiers.

ISO/IEC 18013-5, developed originally for mobile driving licenses (mDL), defines a CBOR-encoded credential structure optimised for constrained environments where bandwidth, storage, and computational resources are limited. The mdoc format has been extensively tested and deployed in multiple jurisdictions worldwide, providing a mature foundation for the EUDI Wallet's proximity presentation requirements. Its support for offline verification, enabling credential validation without internet connectivity, is critical for use cases such as border control, retail age verification, and access to physical spaces where network reliability cannot be guaranteed.

The ARF specifies that PID attestations and Qualified Electronic Attestations of Attributes (QEAA) must be issued in accordance with both data models: using Selective Disclosure JSON Web Tokens (SD-JWT) for W3C-based encoding and ISO/IEC 18013-5 mdoc format for CBOR-based encoding. This dual issuance ensures that credentials can be presented in contexts favouring either remote online verification or proximity offline scenarios, maximising usability across the diverse landscape of European digital services [5].

To support semantic interoperability, the ARF introduces attestation rulebooks that define the structure, mandatory and optional attributes, data types, and namespace identifiers for specific credential types. The PID Rulebook, for example, specifies the core attributes that all Member States must support for Person Identification Data, along with mechanisms for national extensions that accommodate legal or administrative specificities. This controlled vocabulary approach reduces ambiguity in credential interpretation and enables automated processing by Relying Parties without requiring manual mapping or translation between national implementations [18].

2.3.2 Protocol Flows for Issuance and Presentation. Standardised protocols for credential issuance and presentation are essential for interoperability between Wallet Instances, PID Providers, Attestation Providers, and Relying Parties. The ARF specifies distinct protocol families depending on the interaction model and technical context.

For remote online credential issuance, the ARF mandates the use of OpenID for Verifiable Credential Issuance (OpenID4VCI), an extension of the OAuth 2.0 and OpenID Connect frameworks designed specifically for issuing verifiable credentials to digital wallets [5]. OpenID4VCI defines how a wallet requests credentials from a PID Provider or Attestation Provider, how the issuer authenticates the user and verifies their eligibility, and how cryptographic holder binding is established to ensure credentials cannot be transferred to unauthorised parties. The protocol supports both synchronous issuance, where credentials are delivered immediately upon successful authentication, and deferred issuance, where background verification processes complete before credential delivery.

For remote online credential presentation, the ARF specifies OpenID for Verifiable Presentations (OpenID4VP), which enables Relying Parties to request specific attributes from a wallet and receive cryptographic proofs of credential authenticity and holder control [5]. OpenID4VP leverages presentation exchange protocols that allow Relying Parties to express fine-grained attribute requests, enabling selective disclosure aligned with data minimisation requirements. The protocol includes mechanisms for mutual authentication, ensuring that both the wallet and the Relying Party can verify each other's legitimacy before exchanging sensitive information.

For proximity presentation scenarios, the ARF adopts the ISO/IEC 18013-5 device engagement and data retrieval protocols, which define how a secure communication channel is established between the wallet and a verifier using NFC, Bluetooth Low Energy, or QR codes [5]. These protocols support offline verification, where the verifier validates credential signatures and revocation status using locally cached issuer certificates and cryptographic material, without requiring real-time network access. The proven deployment of ISO/IEC 18013-5 in mobile driving license programmes across multiple countries provides confidence in its reliability for high-assurance offline verification scenarios.

The combination of OpenID-based protocols for online interactions and ISO/IEC 18013-5 protocols for proximity use cases ensures that the EUDI Wallet can operate across the full spectrum of digital identity transactions, from remote authentication to e-government services to in-person verification at border checkpoints or retail establishments [18].

2.3.3 Trust Infrastructure and Recognition. Cross-border interoperability depends not only on common data formats and protocols but also on a trust infrastructure that enables verifiers to validate

credentials issued by providers in other Member States. The ARF establishes a hierarchical trust model anchored through qualified trust service providers operating under eIDAS 2.0 supervision, trust registries maintained at national and European levels, and mechanisms for certificate validation and revocation checking [5, 9].

For ISO/IEC 18013-5-based credentials, trust is established through an X.509 Public Key Infrastructure (PKI) where each PID Provider and Attestation Provider operates as a certificate authority with its own root certificate. National trust registries publish issuer metadata, certificate chains, and revocation information, enabling Relying Parties to retrieve the cryptographic material necessary to verify credential signatures and validate issuer authenticity. The trust registries themselves are discoverable through standardised protocols, and their integrity is protected through cryptographic signatures from national supervisory authorities [9, 18].

For W3C-based credentials using SD-JWT, the ARF specifies trust frameworks based on OpenID Federation, which provides a distributed trust model enabling entities to establish trust relationships through cryptographic proofs and metadata exchanges. OpenID Federation supports hierarchical trust chains where intermediate entities vouch for leaf entities, enabling scalable trust propagation across the EU ecosystem without requiring pre-negotiated bilateral agreements. Trust anchors at the European level, maintained by the European Commission or designated EU-wide trust service providers, provide ultimate roots of trust that Member States and sectoral services can rely upon [5].

The trust infrastructure also incorporates mechanisms for certificate and credential revocation, ensuring that compromised or expired credentials cannot be used for fraudulent purposes. Revocation status can be checked through Online Certificate Status Protocol (OCSP) queries, Certificate Revocation Lists (CRLs), or more privacy-preserving mechanisms such as status list credentials that enable batch revocation checking without revealing which specific credentials are being validated. The ARF requires that Wallet Instances check revocation status before presenting credentials to Relying Parties, and that Relying Parties verify revocation status as part of their credential validation process [5].

Crucially, the legal framework of eIDAS 2.0 mandates mutual recognition of credentials issued under the regulation, meaning that a PID issued in one Member State must be accepted by Relying Parties in all other Member States [18, 19]. This legal obligation, combined with the technical interoperability mechanisms provided by the ARF, eliminates historical fragmentation where national eID schemes operated in isolation and were not recognised across borders. The attestation rulebooks and schema catalogues published by the European Commission provide additional guidance, ensuring that issuers and verifiers interpret credential attributes consistently and that sectoral use cases can be supported through standardised credential types.

The Large-Scale Pilots (LSPs) currently underway across Europe, including the POTENTIAL consortium involving 19 Member States and over 140 partners, provide real-world validation of these interoperability mechanisms. Pilot participants are testing credential issuance, presentation, and verification flows across diverse implementations, identifying integration challenges and refining specifications to ensure seamless operation when the EUDI Wallet is mandated for all Member States by the end of 2026 [5].

3 Pilot Test Implementation

To evaluate the practical implementation and operational workflow of an EUDI Wallet based on the eIDAS 2.0 framework [17], we developed a comprehensive pilot test. The eIDAS 2.0 regulation, adopted by the European Parliament on 29 February 2024 and entered into force on 20 May 2024, mandates all EU member states to offer their citizens EUDI Wallets by the beginning of 2027. This pilot simulates a real-world scenario involving three fundamental ecosystem components as defined in the EUDI Wallet Architecture and Reference Framework (ARF) [1]: a User Wallet, an Issuer, and a Verifier.

The scenario demonstrates the complete lifecycle of a digital academic credential: a university (Issuer) issues a diploma, which is securely stored in the student's wallet, and later presented to an employer or institution (Verifier) to prove academic qualifications. All components were built using EU reference codebases [2], adapted specifically for this demonstration.

3.1 System Architecture and Configuration

The entire architecture was deployed on a single Windows 11 machine, allowing for complete local testing of the ecosystem while maintaining the distributed nature of the components as described in the ARF [1].

3.1.1 User Wallet Configuration. The User Wallet implementation leverages the official Android reference application from the `eudi-app-android-wallet-ui` repository [3]. We used Android Studio both for source code modifications and to run the application through its integrated device emulator. This approach provided a realistic mobile environment without requiring physical hardware during development and testing phases. The wallet implements the core functionalities mandated by Article 5a of the eIDAS 2.0 regulation [17].

3.1.2 Issuer Service Setup. The Issuer service runs as a Flask-based web application developed in Python 3.11. Using Visual Studio Code as the development environment, we configured the service to operate on `localhost:5000`, making it accessible to the User Wallet for credential issuance requests. The implementation draws from the official `eudi-srv-web-issuing-eudiw-py` repository [4], with all required dependencies managed through a `requirements.txt` file. The issuer follows the OpenID for Verifiable Credential Issuance (OpenID4VCI) protocol [11] as specified in the ARF.

3.1.3 Verifier Service Architecture. The Verifier operates as a RESTful backend implementing the OpenID for Verifiable Presentations (OpenID4VP) 1.0 protocol [12], serving as the trusted Relying Party endpoint as defined in Article 5b of the eIDAS 2.0 regulation [17]. OpenID4VP defines a mechanism on top of OAuth 2.0 that enables presentation of Verifiable Credentials as Verifiable Presentations. Built with Angular, it exposes two distinct API surfaces as prescribed by the ARF [1]:

The **Verifier API** manages the verification lifecycle, handling transaction initialization for Self-Issued OpenID Provider v2 (SIOPv2), OpenID4VP, or hybrid authentication requests [12], and processing both successful and error responses from the User Wallet.

The **Wallet API** facilitates bidirectional communication with the User Wallet. It provides a *Get Requested Object* endpoint that

delivers metadata via JWT-secured authorization, and a *Post to Wallet* endpoint that enables the Wallet to generate authorization tokens for subsequent data presentation requests.

3.2 End-to-End Workflow

The pilot test follows a logical sequence that mirrors real-world credential usage within the EUDI Wallet ecosystem [1]:

(1) The user navigates to the Issuer's web portal and initiates a request for an academic diploma credential conforming to the W3C Verifiable Credentials Data Model [20].
(2) The Issuer authenticates the user through established credentials (such as institutional username and password) and verifies their eligibility to receive the diploma credential based on academic records, following the attestation issuance procedures defined in the ARF [1].
(3) Upon successful verification, the Issuer constructs a Verifiable Credential containing the diploma data according to the W3C standard [20], cryptographically signs it with its private key, and transmits it securely to the User Wallet using the OpenID4VCI protocol [11].
(4) The User Wallet receives and stores the credential in its secure storage mechanism, leveraging the Wallet Secure Cryptographic Device (WSCD) as specified in the ARF [1], making it available for future presentations.
(5) When the user needs to prove their academic qualification, they initiate a verification session with the Verifier, following the attestation presentation flows defined in the ARF [1].
(6) The Verifier generates a QR code containing the presentation request parameters conforming to the OpenID4VP protocol [12], which the user scans using their Wallet application.
(7) The Wallet retrieves the associated metadata from the verification request, understanding what information the Verifier requires based on the presentation definition or DCQL query [12].
(8) The user reviews the request and selects the appropriate credential—in this case, the academic diploma—exercising their right to control which data is shared as guaranteed by the eIDAS 2.0 framework [17].
(9) The Wallet constructs a Verifiable Presentation tailored to the Verifier's requirements, following the W3C Verifiable Credentials Data Model [20] and the OpenID4VP protocol [12].
(10) The Verifier performs comprehensive validation as mandated by the ARF [1], checking cryptographic signatures, verifying credential integrity, confirming the Issuer's trust status within the EUDI Trust Infrastructure [6], validating expiration and issuance timestamps, and ensuring full conformance with the OpenID4VP protocol [12].
(11) Upon successful validation of all security and trust parameters, the Verifier provides confirmation to the user, completing the verification process in accordance with the relying party requirements specified in Article 5b of the eIDAS 2.0 regulation [17].

3.3 Technical Deep Dive

This section explores the technical implementation details, security mechanisms, and protocol-level operations of each component as defined by the ARF [1] and relevant technical standards.

3.3.1 Issuer: Credential Generation and Cryptographic Signing. The Issuer orchestrates several critical operations to produce a secure, verifiable credential compliant with both the W3C Verifiable Credentials Data Model [20] and the OpenID4VCI protocol [11].

Data Processing and Structuring. When a request arrives, the Issuer first authenticates the user and retrieves the relevant academic records from its internal database. It then transforms this institutional data into the standardized W3C Verifiable Credential data model, ensuring interoperability with any compliant wallet or verifier. This transformation maps diploma attributes—such as degree type, field of study, graduation date, and honors—into the structured credential format. The credential structure includes metadata fields such as `@context`, `type`, `issuer`, `issuanceDate`, `credentialSubject`, and `proof` as specified in the W3C standard [20].

Cryptographic Operations. Security is established through asymmetric cryptography conforming to the security requirements defined in the ARF [1]. The Issuer signs the credential using its private key, typically employing ECDSA (Elliptic Curve Digital Signature Algorithm) or EdDSA (Edwards-curve Digital Signature Algorithm) algorithms. The corresponding public key is published through the EUDI Trust Infrastructure [6], allowing any verifier to validate the signature's authenticity. Each credential includes a comprehensive `proof` block containing the signature value, a key identifier (KID) referencing the specific signing key, the algorithm used, an issuance timestamp, and a reference to the credential schema as prescribed by the W3C Verifiable Credentials Data Model [20].

Secure Transmission. The signed credential is transmitted to the User Wallet over HTTPS, ensuring confidentiality and integrity during transit. Following the OpenID4VCI protocol [11], the credential may be packaged as either a JWT-VC (JSON Web Token format) or a COSE/CBOR object, both widely supported standards in the digital identity space and accepted formats within the EUDI Wallet ecosystem [1].

3.3.2 User Wallet: Secure Storage and Presentation Logic. The Wallet serves as the user's personal credential repository and presentation agent, requiring robust security at every layer as mandated by the ARF [1].

Storage Security Architecture. The wallet implements a Cryptographic Keys Management System responsible for managing and storing cryptographic information, including private keys generated during the credential issuance process. Credentials reside in the Android Keystore, which provides hardware-backed encryption on supported devices. Critically, the user's private keys never leave the device and cannot be extracted or backed up, ensuring compliance with the WSCD requirements defined in the ARF [1]. Accessing stored credentials requires active user consent, typically enforced through biometric authentication or PIN entry, preventing unauthorized access even if the device is compromised.

Credential Management. The Wallet maintains complete Verifiable Credentials as received from Issuers, preserving all claims and metadata in accordance with the W3C Verifiable Credentials Data Model [20]. When a presentation request arrives via the OpenID4VP protocol [12], the Wallet parses the metadata—often structured as JWT or Selective Disclosure JWT (SD-JWT)—to understand exactly what the Verifier requires. The Attestation Exchange Protocol defines how to request and present credentials in a secure and privacy-preserving fashion. It then constructs a Verifiable Presentation containing only the necessary attributes, implementing the principle of data minimization as guaranteed by the eIDAS 2.0 regulation [17].

Presentation Security. Each Verifiable Presentation is signed with the user's private key, cryptographically binding it to the wallet holder. For credentials that support selective disclosure, the Wallet can reveal only requested attributes while keeping others hidden, a key privacy feature of the EUDI Wallet ecosystem [1]. To prevent replay attacks, each presentation incorporates unique nonce and state parameters provided by the Verifier as specified in the OpenID4VP protocol [12], ensuring the presentation cannot be intercepted and reused.

3.3.3 Verifier: Multi-Layer Validation Framework. The Verifier implements a defense-in-depth approach, performing checks at the cryptographic, structural, trust, and protocol levels as mandated by Article 5b of the eIDAS 2.0 regulation [17] and the ARF [1].

Initial Processing. The Verifier receives the Verifiable Presentation through an OpenID4VP channel—either as a redirect or POST request. It extracts the embedded Verifiable Credential(s) and validates the structural integrity, ensuring compliance with the expected schemas defined in the W3C Verifiable Credentials Data Model [20] and data formats specified in the ARF [1].

Cryptographic Verification. Both the Verifiable Presentation and the underlying Verifiable Credential undergo signature verification following the cryptographic requirements specified in the ARF [1]. The Verifier retrieves the Issuer's public key from trusted metadata sources within the EUDI Trust Infrastructure [6] and confirms that the signatures are valid and unaltered. It also validates temporal parameters as defined in the OpenID4VP protocol [12], checking that nonce values match, state parameters are correct, credentials haven't expired, and issuance dates are reasonable.

Trust Framework Integration. Beyond cryptographic validity, the Verifier must establish trust in the Issuer through the EUDI Trust Infrastructure [6]. It confirms that the Issuer is a recognized, trusted entity within the EUDI ecosystem, validates that the credential type and format are permitted for the requested purpose, and checks revocation status against any configured revocation lists or status endpoints as specified in the ARF [1].

Authorization Decision. After completing all validation layers mandated by the eIDAS 2.0 regulation [17] and the ARF [1], the Verifier makes its final determination. Success results in a confirmation message delivered to the user. Failure triggers a standardized error response conforming to the OpenID4VP protocol [12]—such as `invalid_signature`, `expired_credential`, or `issuer_not_trusted`—providing clear feedback about why the verification failed while maintaining security by not revealing sensitive details to potential attackers.

4 Conclusion

This report analysed how specific components of the EUDI ARF support secure and privacy-preserving digital identity transactions and proposed a high-level pilot design to illustrate their application in practice. By structuring the discussion around identity verification, data minimisation, and interoperability, we highlighted the architectural strengths of the framework and the main trade-offs involved in real-world deployments. The pilot design showed how these components can be orchestrated in a concrete use case, offering a starting point for further technical refinement and implementation work.

Acknowledgments

The authors would like to acknowledge the work of the European Commission and the Member State experts involved in the definition of the EUDI Architecture and Reference Framework, as well as the broader research and standards communities working on digital identity and privacy-enhancing technologies.

References

[1] European Commission. 2024. Architecture and Reference Framework for the European Digital Identity Wallet. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/. Version 1.6, European Digital Identity Wallet Consortium.

[2] European Commission. 2024. EU Digital Identity Wallet Reference Implementation. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/. European Digital Identity Wallet Consortium.

[3] European Commission. 2024. EUDI Wallet Reference Implementation - Android Wallet UI. https://github.com/eu-digital-identity-wallet/eudi-app-android-wallet-ui.

[4] European Commission. 2024. EUDI Wallet Reference Implementation - Web Issuing Service (Python). https://github.com/eu-digital-identity-wallet/eudi-srv-web-issuing-eudiw-py.

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

[6] European Commission. 2024. Trust Framework for the European Digital Identity Wallet Ecosystem. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/. Annex to the Architecture and Reference Framework.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] OpenID Foundation. 2024. OpenID for Verifiable Credential Issuance. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html. OpenID Specification.

[12] OpenID Foundation. 2024. OpenID for Verifiable Presentations - draft 1.0. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html. OpenID Specification.

[13] 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.

[14] 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.

[15] 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.

[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 Article emphasising that the EUDI Wallet aims to ensure personal data sovereignty; credentials are stored in a decentralised wallet controlled by the user.

[17] European Parliament and Council of the European Union. 2024. Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401183. Official Journal of the European Union, L 2024/1183, May 2024.

[18] 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.

[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.

[20] World Wide Web Consortium (W3C). 2025. Verifiable Credentials Data Model v2.0. https://www.w3.org/TR/vc-data-model-2.0/. W3C Recommendation, May 2025.