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 3 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

Identity Proofing and PID Issuance.

Authentication of the Holder.

Mutual Authentication with Relying Parties.

2.2 Data Minimisation and Consent Management

Selective Disclosure of Attributes.

User Consent and Transparency.

Unlinkability and Anti-Tracking Measures.

2.3 Interoperability Mechanisms

Cross-Border Credential Formats.

Protocol Flows for Issuance and Presentation.

Trust Infrastructure and Recognition.

3 Pilot Design

Based on the component evaluation in Section 2, this section outlines a minimally functional pilot design for a specific use case. The goal is not to specify an implementation in full technical detail, but to demonstrate how identity attributes, trust flows, and privacy safeguards defined in the ARF can be combined in a realistic scenario.

3.1 Use Case Description

3.2 Actors and ARF Components

3.3 Flow of Identity Attributes and Trust

3.4 Security, Privacy, and Interoperability Considerations

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