

Trust at Infrastructure Scale: Cryptographic Architecture and Resilience Engineering for the EU Digital Identity Wallet

Veelasha Moonsamy

ORCID: 0000-0001-6296-2182

Horst Görtz Institute for IT Security, Ruhr University Bochum, Bochum, Germany

Hamid Bostani

ORCID: 0000-0002-2097-5521

Digital Security Group, Institute for Computing and Information Sciences, Radboud University, Nijmegen, Netherlands

Correspondence: Veelasha Moonsamy · contact details held in the journal record

Publication history. Assigned by the publisher to Cybersecurity Advances, Volume 2, Issue 1 (2025). This publisher-authorized digital edition was released on 29 October 2026 from the supplied final 2025 manuscript. Review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized; substantive scholarly content was preserved.

© 2025 the author(s). Published by AlphaTech Scholarly Press under the Creative Commons Attribution 4.0 International License (CC BY 4.0). No DOI is displayed unless and until registration is independently verified.

Background: eIDAS 2.0 (Regulation (EU) 2024/1183, in force 20 May 2024) obliges every member state to offer citizens a European Digital Identity Wallet (EUDI Wallet) by the end of 2026. The regulatory build-out ran on schedule through 2025: five implementing regulations on core functionalities and interfaces (December 2024), and seven further trust-services regulations plus an electronic-attestations regulation (July 2025) — the largest deployment of verifiable-credential infrastructure ever attempted. **Objective:** We analyze the wallet's cryptographic architecture and its resilience-engineering requirements: what must hold for a credential infrastructure at the scale of 450 million residents to be trustworthy, and which failure classes its design must survive. **Methods:** Documentary analysis of the regulation, the implementing regulations, and the underlying open standards (W3C Verifiable Credentials 2.0, ISO/IEC 18013-5 mobile driving licence, SD-JWT-class selective disclosure); construction of an ecosystem architecture model; and a risk-versus-mechanism coverage assessment. **Results:** The wallet's trust model distributes cryptographic authority across issuers, holders, and registered relying parties — an architectural inversion of centralized identity that removes the standing honeypot but creates a new resilience surface: revocation latency, verifier over-collection, certification gaps between wallet solutions, and cross-border interoperability failures. The 2025 implementing regulations address the governance layer (trust services, attestations) but leave the operational-resilience layer — revocation infrastructure guarantees, ecosystem-scale incident response — as open engineering work. **Conclusions:** Digital identity at infrastructure scale is the decade's most consequential trust build; its security will be decided less by cryptography (which is largely settled) than by operational resilience engineering — revocation with guarantees, recovery with rehearsals, transparency for components that fail silently, and the humility to keep manual fallbacks while the ecosystem itself is the newest and least-tested component.

Keywords: digital identity; eIDAS 2.0; European Digital Identity Wallet; verifiable credentials; selective disclosure; trust infrastructure; resilience engineering; digital trust

Contribution statement. This paper makes four contributions: (1) a source-verified account of the EUDI Wallet's 2024-2025 regulatory build-out and its 2026 deadline; (2) an ecosystem architecture model identifying the trust relationships and their governance layer; (3) an analysis of the wallet's core cryptographic building blocks and the resilience properties they imply; and (4) a risk-versus-mechanism coverage assessment identifying the operational-resilience gaps that remain open engineering work for 2026.

1. Introduction

Digital identity has been the European Union's most ambitious infrastructure project of the decade. Regulation (EU) 2024/1183 — the eIDAS 2.0 amendment — entered into force on 20 May 2024 and requires every member state to provide at least one **European Digital Identity Wallet** to citizens by the end of 2026 [1]. The wallet is conceived as more than login: it will carry personal identification data (PID), diplomas, attestations, qualified electronic signatures, and sectoral credentials, usable across borders for public and private services. In engineering terms, the EU is deploying a **verifiable-credential infrastructure at the scale of a**

continent — issuers in every member state, wallets on every citizen's device, registered relying parties in every sector — with mandatory interoperability and privacy-preserving disclosure.

2025 was the year the regulatory substrate solidified. In December 2024, the Commission adopted the first five implementing regulations, laying down the wallet's core functionalities, its protocols and interfaces, and certification rules [2]. In July 2025, a second wave followed: seven implementing regulations focused on trust services, plus one detailing electronic attestations of attributes — published in the Official Journal on 29-30 July 2025 and entering into force twenty days thereafter [3]. By year-end 2025, the legal architecture for the 2026 wallet deadline was substantially in place, and the engineering question had changed character: less "what is the cryptography?" (largely settled across the standards landscape) and more "how does a credential ecosystem of this scale fail, and what does resilience engineering look like for it?" [1][2][3].

1.1 Research questions

RQ1: What is the verified 2024-2026 regulatory build-out, and what does its pace imply for implementers? **RQ2:** What is the wallet ecosystem's architecture, and how does its trust distribution differ from centralized identity? **RQ3:** What are the wallet's core cryptographic building blocks, and which resilience properties do they imply? **RQ4:** Which risk classes remain open engineering work as the 2026 deadline arrives?

1.2 Contributions

(1) The verified regulatory build-out record (Section 2, Figure 1, Table 1) (RQ1). (2) The ecosystem architecture model (Section 3, Figure 2) (RQ2). (3) The cryptographic building-block analysis (Section 4, Table 2) (RQ3). (4) The risk-versus-mechanism coverage assessment (Section 5, Figure 3, Table 3) (RQ4).

2. The Regulatory Build-Out (RQ1)

Figure 1 and Table 1 present the sequence. The pace is the finding: between the framework regulation (May 2024) and the second implementing-regulation wave (July 2025), the EU specified the wallet's core functionality, protocols and interfaces, certification, trust-service integration, and attestations — a regulatory engineering cycle that would typically span a decade compressed into eighteen months [1][2][3]. For implementers, the consequence is a compressed design-freeze horizon: wallet solutions entering certification in 2025-2026 are building against specifications that finalized in the same window. The December 2026 deadline for member-state wallet provision then functions as the ecosystem's first operational milestone — the moment the newest, least-tested component of European digital infrastructure becomes a citizen-facing service.

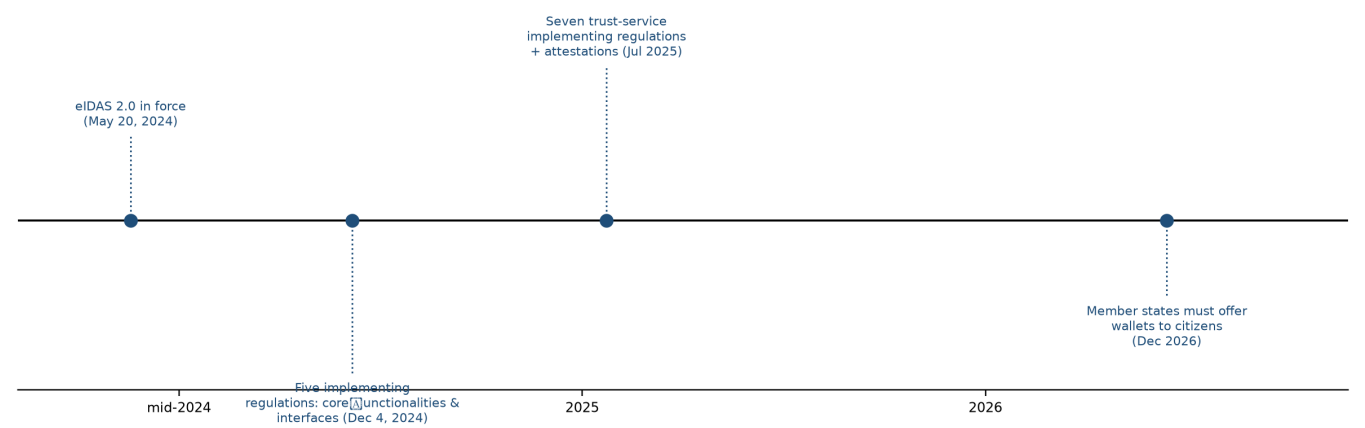


Figure 1. The EUDI Wallet regulatory build-out, 2024-2026 [1][2][3].

Milestone	Date	Content	Source
eIDAS 2.0 in force	May 20, 2024	Regulation (EU) 2024/1183: wallet obligation, framework, governance	[1]
First implementing-regulation wave	Dec 4, 2024	Five regulations: core functionalities, protocols & interfaces, certification (C(2024) 8495, C(2024) 8496, et seq.)	[2]
Second implementing-regulation wave	Jul 2025	Seven trust-service regulations + one electronic-attestations regulation; OJ publication Jul 29-30, 2025; in force 20 days thereafter	[3]

Wallet provision deadline	End of 2026	Every member state must offer at least one EUDI Wallet to citizens	[1]
---------------------------	-------------	--	-----

Table 1. The EUDI Wallet regulatory build-out, 2024-2026 [1][2][3].

3. The Ecosystem Architecture (RQ2)

Figure 2 presents the model. Three roles and a governance layer. **Issuers** (member states, PID providers, and attestation issuers) cryptographically bind credentials to holders. **The wallet** (the holder's device application) stores credentials, enforces selective disclosure, and signs presentations with device-secured keys. **Relying parties** (registered verifiers) request presentations for stated purposes and are subject to registration and data-protection duties — the architecture's deliberate answer to the over-collection problem. The **governance layer** — the regulation (which extends the original eIDAS trust-service framework to wallet credentials [5]), the implementing acts, the registry of trusted issuers, wallet certification, and revocation infrastructure — is what makes the tripartite trust work at borders: the credential a German issuer signs must verify in a Portuguese relying party's context, under rules neither party administers [1][2][3].

The architectural inversion deserves emphasis. Centralized identity concentrates authentication at a provider (the standing honeypot problem); the wallet distributes it to cryptographic issuers and holder-held credentials. This removes the honeypot but multiplies the *number of independently operating components* whose failures matter: every issuer's compromise, every wallet solution's defect, every relying party's over-collection now events in a shared ecosystem. Resilience engineering, not perimeter design, is the discipline the architecture calls for.

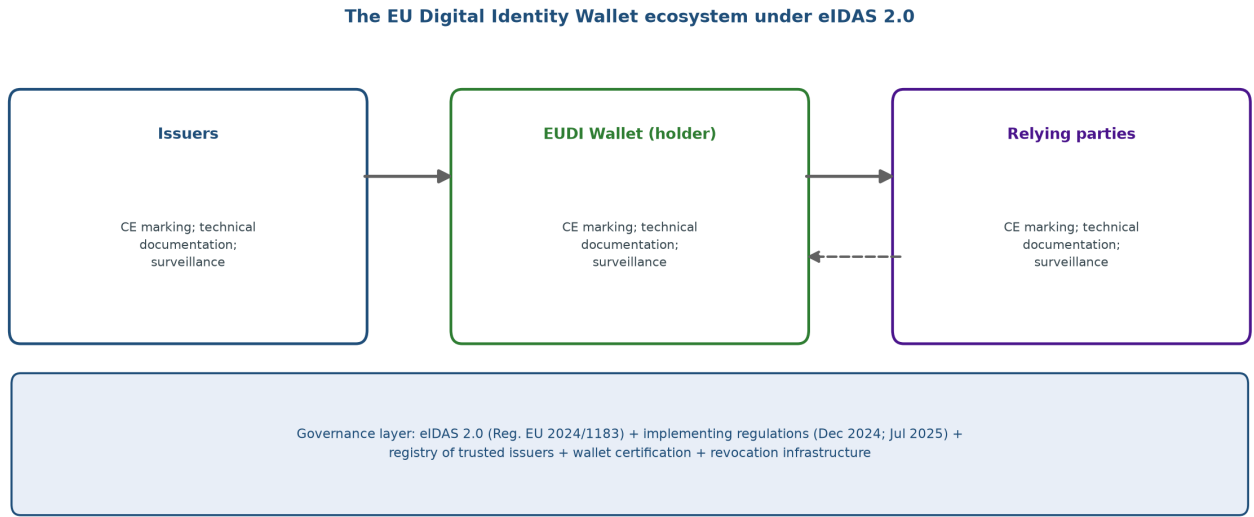


Figure 2. The EUDI Wallet ecosystem: issuers, the holder-controlled wallet, registered relying parties, and the governance layer [1][2][3][5].

4. Cryptographic Building Blocks (RQ3)

Table 2 summarizes the core building blocks and their resilience properties.

Verifiable credentials. The wallet's unit of trust is the verifiable credential — a cryptographically signed attestation, with W3C's Verifiable Credentials Data Model 2.0 finalized in 2025 as the interoperability target [4]. The credential's signature lets a relying party verify issuer authenticity *offline* — an architectural resilience property: verification does not require the issuer's availability, only its registered key material.

Selective disclosure. The privacy-preserving core: presenting a single attribute (age over 18) without disclosing the full credential. The implementing regulations standardize the SD-JWT and mdoc/mDL class mechanisms [2][3][6][8], and the choice carries resilience implications — unlinkability across presentations constrains revocation design, and vice versa.

Device-secured keys and holder binding. Wallet keys live in device secure elements; holder binding is the mechanism that makes a stolen wallet a recoverable event rather than an identity takeover, consistent with the assurance levels digital-identity guidance revised in the same window prescribes [7]. Key-recovery and re-issuance workflows are therefore resilience-critical components, not UX details.

Revocation infrastructure. The least-glamorous and most operationally demanding block: a revocation/status mechanism must be fast (revoked credentials must stop verifying promptly), privacy-preserving (status checks must not enable holder tracking), and *itself* resilient — it is the component whose outage either freezes verification or silently extends the life of revoked credentials [3] [6].

Building block	Function	Resilience property / implication
Verifiable credentials (W3C VCDM 2.0)	Signed, interoperable attestations	Offline verification; issuer availability is not on the verification path
Selective disclosure (SD-JWT / mdoc classes)	Attribute-level presentation	Unlinkability constrains revocation design (and vice versa)
Device-secured holder keys	Holder binding; presentation signing	Stolen wallet is a recoverable event if re-issuance workflows are engineered
Revocation / status infrastructure	Timely invalidation of compromised credentials	Must be fast, privacy-preserving, and itself resilient - the least-glamorous critical block
Registered relying parties	Purpose-bound verification duties	Architectural answer to over-collection; enforcement is the open question
Wallet certification	Common core across heterogeneous wallet solutions	Partial cover for inter-solution gaps; large-scale pilots as proving ground

Table 2. Core cryptographic building blocks of the wallet architecture [2][3][4][6].

5. Risk Classes and Coverage (RQ4)

Figure 3 and Table 3 assess six risk classes against six mitigation mechanisms. Three findings. **Issuer and registry compromise** (R1) is the ecosystem's highest-value target; selective disclosure and hardware-backed storage provide partial cover, and the strong residual need is registry governance and incident transparency. **Verifier over-collection** (R3) is the privacy failure mode the architecture was built to prevent; purpose-bound registered relying parties score strong as designed, but enforcement in the wild is the open question. **Revocation latency** (R4) and **cross-border interoperability** (R5) are the operational-resilience gaps the 2025 regulations addressed least; both are 2026 engineering work. **Certification gaps between wallet solutions** (R6) — heterogeneous implementations certified against a common core — are partially addressed by the implementing regulations, with the large-scale pilots as the remaining proving ground.

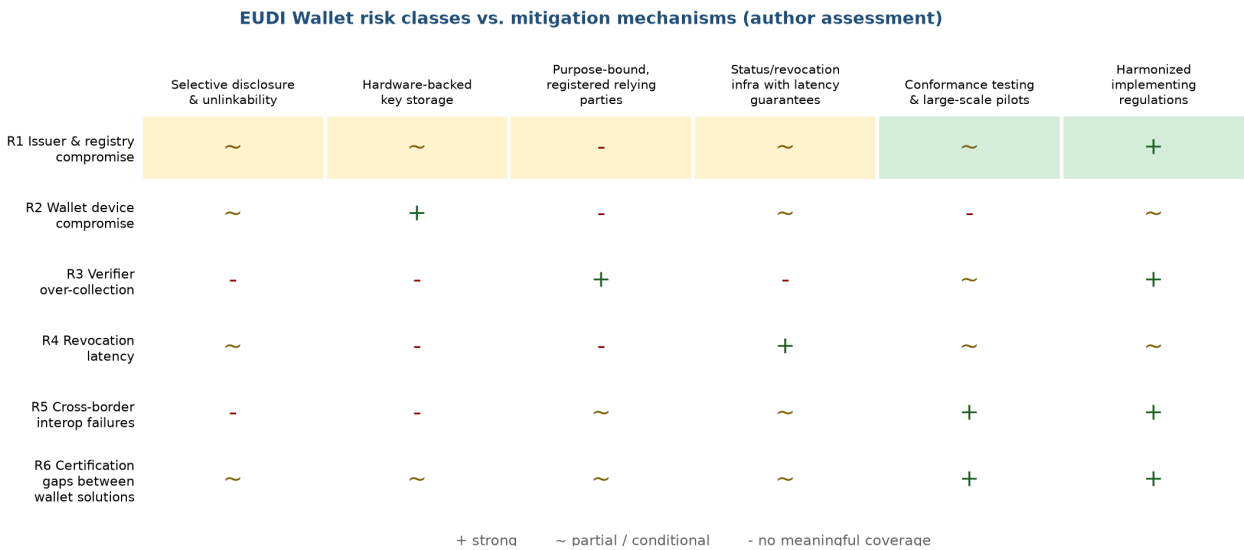


Figure 3. EUDI Wallet risk classes versus mitigation mechanisms (author assessment; register detail in Table 3).

Risk class	Description	Strongest mitigation	Residual gap
R1 Issuer & registry compromise	Compromise of a member-state issuer or the trusted-issuer registry	Registry governance; transparency	Ecosystem-scale incident response

R2 Wallet device compromise	Device-level theft/malware against holder keys	Hardware-backed key storage; re-issuance	Recovery UX at population scale
R3 Verifier over-collection	Relying parties requesting beyond stated purpose	Registered, purpose-bound relying parties	Field enforcement
R4 Revocation latency	Revoked credentials remain verifiable too long	Status infrastructure with latency guarantees	Ecosystem-wide SLAs not yet specified
R5 Cross-border interoperability failures	Credentials failing in other member states' contexts	Conformance testing; large-scale pilots	Divergent national implementations
R6 Certification gaps	Heterogeneous wallet solutions certified against a common core	Harmonized implementing regulations	Pilot coverage of real-world flows

Table 3. Wallet risk classes, mechanisms, and residual gaps (author assessment).

6. Resilience Engineering for the Wallet Ecosystem

Four requirements follow from the coverage assessment. **Manual fallbacks are architecture, not regression:** for the first years of a credential ecosystem, the ability to transact *without* the wallet is a resilience property; decommissioning legacy channels prematurely converts ecosystem incidents into citizen lockouts. **Revocation transparency:** status-infrastructure incidents must be detectable by relying parties — a silent revocation failure is worse than a loud one. **Ecosystem incident response:** the governance layer needs a practiced procedure for issuer compromise, wallet-solution defects, and registry incidents — at the speed the 24/72-hour reporting culture of neighboring regimes (NIS2, the CRA) has normalized. **Measured rollout:** the 2026 deadline is a *provision* deadline; resilience argues for credential-class-by-credential-class expansion (PID first, high-value attestations later) so that each ecosystem failure is discovered while the blast radius is still bounded.

7. Limitations and Threats to Validity

Construct validity. The six risk classes are an analytical cut of a moving regulatory target; later implementing acts may re-classify mechanisms. **Internal validity.** The coverage assessments are author judgments; specific wallet certifications and pilot outcomes will supersede them. **External validity.** The analysis addresses the EU wallet ecosystem as specified through 2025; national implementations will diverge in the details that resilience actually depends on (recovery procedures, revocation services). **Temporal scope.** Frozen at year-end 2025, before the 2026 provision deadline and the certification cycle's first results.

8. Conclusion

The EU Digital Identity Wallet is the largest deliberate trust-infrastructure deployment ever attempted: cryptographic authority distributed to 27 member states' issuers, credentials in hundreds of millions of devices, and relying parties across every sector, by the end of 2026. Its cryptography is largely settled; its governance moved remarkably fast; what remains is the discipline this paper has argued for — operational resilience engineering for the ecosystem itself: revocation with guarantees, recovery with rehearsals, transparency for the components that fail silently, and fallbacks that keep citizens whole while the newest component of European digital infrastructure grows up. Digital trust at infrastructure scale is not a property any single actor can confer; it is what the ecosystem demonstrates, incident by handled incident, from 2026 onward.

Declarations

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CRediT contribution statement. Veelasha Moonsamy: conceptualization, privacy and credentials analysis, writing – original draft. Hamid Bostani: validation, cryptographic architecture analysis, writing – review & editing. (Corresponding author: Veelasha Moonsamy.)

Competing interests. The authors declare no competing interests.

Data and code availability. No new datasets were generated; all regulatory claims trace to the cited official sources [1][2][3].

Ethics and dual-use. Not applicable; the paper contains no offensive content.

AI assistance declaration. AI-based tools were used in a limited supporting capacity (literature search, figure preparation, and language editing); all research content, analysis, and conclusions were produced, reviewed, and verified by the authors, who take full responsibility for the work.

References

- [1] Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 (eIDAS 2.0) as regards establishing the European Digital Identity Framework, OJ L, 20 May 2024 (member states to provide wallets by the end of 2026).
- [2] European Commission, "Implementing regulation for European Digital Identity Wallets - five implementing regulations adopted (C(2024) 8495, C(2024) 8496, et seq.)," Dec. 4, 2024. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-european-digital-identity-wallets>
- [3] European Commission, "New round of EU Digital Identity Wallet implementing regulations adopted (seven trust-service regulations; one electronic-attestations regulation)," Jul. 2025. [Online]. Available: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/>
- [4] W3C, "Verifiable Credentials Data Model v2.0," W3C Recommendation, 2025. [Online]. Available: <https://www.w3.org/TR/vc-data-model-2.0/>
- [5] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), OJ L 257, Aug. 2014.
- [6] ISO/IEC 18013-5:2021, Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application. International Organization for Standardization, 2021.
- [7] NIST, "Digital Identity Guidelines," NIST SP 800-63 Revision 4, Aug. 2025. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/63/4/final>
- [8] OpenID Foundation, "SD-JWT-based Verifiable Credentials" (SD-JWT VC), IETF/OpenID specification family, 2025. [Online]. Available: <https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/>