EVALUATING NATIONAL PKI SYSTEMS UNDER eIDAS 2.0: A CROSS-COUNTRY COMPARATIVE ANALYSIS

Alexandru DICEA[1], Ciprian DOBRE[2]

This paper presents a cross-country comparative analysis of public key infrastructure (PKI) systems across seven European Union countries—Estonia, Germany, France, Romania, Italy, Spain, and the Netherlands—within the context of the evolving eIDAS 2.0 regulation. The study aims to understand how each country is preparing for the new digital identity and trust framework, focusing on aspects such as governance, mobile identity adoption, technical standards, cybersecurity, and participation in cross-border blockchain pilots. Using a qualitative, document-based methodology, we evaluate the maturity of national digital identity ecosystems based on a multi-factor index that includes population coverage, usage of electronic signatures, and the density of Qualified Trust Service Providers (QTSPs). Estonia and Germany have achieved advanced integration, while Romania and France demonstrate challenges in policy alignment and infrastructure readiness. The analysis identifies common gaps in interoperability, semantic standards, and cryptographic resilience, especially regarding post-quantum security. The study also summarizes the role of national computer security teams and EU agencies such as ENISA [2] in improving trustworthiness across PKI systems. A forward-looking section outlines the path toward harmonized wallet deployment, metadata alignment, and self-sovereign identity integration. The paper concludes with practical recommendations to accelerate policy coordination and technical upgrades necessary for seamless cross-border identity validation under eIDAS 2.0.

Keywords: eIDAS 2.0, PKI, Digital Identity, QTSP, Interoperability, EU Wallet, Post-Quantum Cryptography, ENISA, Cross-Border Trust

1. Introduction

Public key infrastructure (PKI) plays a central role in establishing digital trust across the European Union. It enables secure authentication, electronic signatures, and document verification, all of which are essential for cross-border digital services. Since 2014, the eIDAS Regulation [1] (EU No. 910/2014) has provided a unified legal foundation for electronic identification and trust services in the EU.

eIDAS 2.0, the proposed revision, is a major upgrade. While the original eIDAS focused primarily on cross-border recognition of national eIDs and qualified trust service providers (QTSPs), eIDAS 2.0 introduces a European Digital Identity

[1] Eng., PhD candidate, POLITEHNICA Bucharest, Romania, e-mail: alex.dicea@upb.ro
[2] Prof., Habil., POLITEHNICA Bucharest, Romania, e-mail: ciprian.dobre@upb.ro

Wallet — a user-centric, interoperable mobile application enabling EU citizens and businesses to store and share digital credentials such as diplomas, licenses, and e-signatures securely across borders [16]. This new framework emphasizes greater flexibility, attribute-level sharing, and compliance with future-proof technologies, including post-quantum cryptography (PQC) and self-sovereign identity (SSI) concepts. It also requires member states to align technical and legal infrastructures to ensure real-time cross-border trust. However, its implementation has varied considerably across member states, both in governance and technical design.

With the upcoming rollout of eIDAS 2.0 and the introduction of the European Digital Identity Wallet, EU countries face a renewed challenge: ensuring that national identity systems can interoperate across borders in a seamless, secure, and user-friendly manner. This study reviews and compares the readiness of seven countries—Estonia, Germany, France, Romania, Italy, Spain, and the Netherlands— which reflect varying governance models, digital maturity levels, and trust service environments.

Our goal is to examine these systems in a structured way and to identify what technical, policy, and cybersecurity changes are needed for full alignment with eIDAS 2.0. The analysis draws on official documents, trusted list data, and national reports, and it incorporates both policy-level and technical perspectives.

2. Methodology and Evaluation Framework

This study uses a document-based comparative approach to assess the current state of national PKI systems in seven EU member states. The countries were selected to represent a diverse range of institutional models and technical implementations of electronic identification.

2.1 Data Sources

Data was collected between January and April 2025. The following primary sources were consulted:

- EU Trusted List Browser [3] for official QTSP listings.
- eIDAS Dashboard for node deployment and metadata compliance.
- European Blockchain Services Infrastructure (EBSI) pilot documentation.
- National digital identity and cybersecurity reports published by agencies such as BSI [4] (Germany), ANSSI [5] (France), and CCN-CERT [6] (Spain).
- Technical documentation from infrastructure providers such as Governikus [8], SK ID Solutions, and IRMA [10].

All data sources were accessed directly and validated against official national and EU publications.

Each country's profile was developed by triangulating policy, technical, and adoption-related indicators to ensure a balanced understanding.

2.2 The Digital Identity Maturity Index (DIMI)

To allow meaningful comparison, we propose a synthetic metric called the **Digital Identity Maturity Index (DIMI)**. This composite index—defined for this study to quantify national readiness for eIDAS 2.0, based on publicly available trust infrastructure indicators—reflects the integration and usability of digital identity systems using three weighted dimensions:

1. ***Digital ID Coverage (50%)***: The percentage of the population with an issued digital identity.
2. ***eSignature Usage (30%)***: The number of qualified electronic signatures used monthly per 1,000 citizens.
3. ***QTSP Density (20%)***: The number of Qualified Trust Service Providers per million inhabitants.

The index is calculated as a weighted average using the following formula:

DIMI = (0.5 × Digital ID Coverage Score) + (0.3 × e-Signature Usage Score) + (0.2 × QTSP Density Score)

Each component is scored on a scale from 1 (low) to 5 (high). This standardizes comparisons despite governance differences.

Estimation of Adoption Trends

To complement static indicators with forward-looking insights, projected adoption values were derived from official datasets and national strategy documents. For Romania, quantitative estimates of digital identity and mobile ID usage were extrapolated from the Digital Economy and Society Index (DESI 2024) [27] and the Romanian Ministry of Research, Innovation and Digitalization (MCID, 2025) [26].

The projections assume a compound annual growth rate (CAGR) of 20–25 % in the number of active digital identities, consistent with the average growth observed among late-adopter EU member states in the DESI dataset. Baseline (2025) and target (2027–2030) figures were aligned with government rollout milestones for the ROeID platform and corresponding integrations with public-service portals. These estimates were incorporated into the Digital Identity Maturity Index (DIMI) to reflect not only current readiness but also anticipated convergence under eIDAS 2.0. The same approach can be replicated for other member states as new datasets become available, ensuring comparability across the European digital identity landscape.

2.3 Evaluation Dimensions

To deepen the analysis, five additional readiness dimensions were defined to assess each country's alignment with eIDAS 2.0:

- ***Governance Model***: Refers to how digital identity and trust services are organized at the national level — centralized (e.g., Estonia), federated (e.g., Germany), or mixed. This impacts agility, oversight, and alignment with EU policy.
- ***Mobile ID Adoption***: The extent to which citizens use mobile-based eIDs or digital wallets for public and private services.
- ***QTSP Ecosystem***: The diversity, accreditation, and operational maturity of Qualified Trust Service Providers in a country (public, private, or mixed ownership of trust providers).
- ***eIDAS Node Deployment***: The technical readiness of a member state's node for cross-border exchange of digital identity attributes.
- ***EBSI Participation***: Engagement in EU-wide initiatives such as the European Blockchain Services Infrastructure or Digital Identity Wallet Consortium.

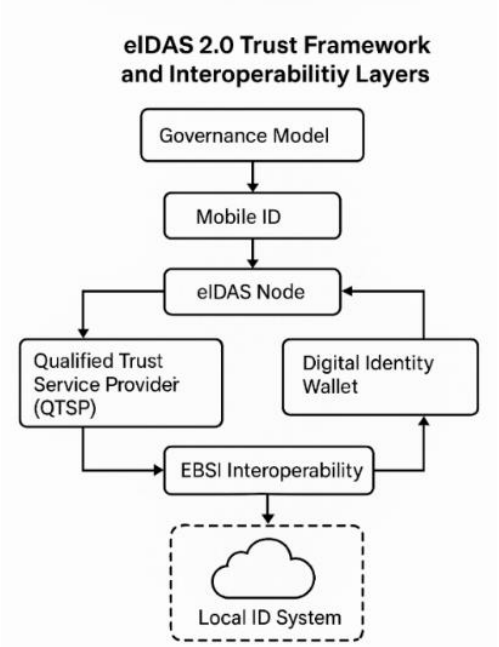

Fig. 1. Architecture of the eIDAS 2.0 trust framework, connecting national identity systems to cross-border services through QTSPs, Wallets, and eIDAS Node.

This diagram illustrates the interaction between national digital identity components (such as QTSPs and mobile IDs), the eIDAS Node, and the European

Digital Identity Wallet. It shows how trust and credential exchange is facilitated across borders via EBSI interoperability, connecting national infrastructures to EU-wide services.

Table 1

PKI Readiness Scores

Country	Governance	Mobile ID	QTSP Diversity	eIDAS Readiness	EBSI Participation
Estonia	5	5	2	5	5
Germany	3	4	4	4	4
France	4	4	5	3	2
Romania	2	2	2	2	1
Italy	3	4	3	4	4
Spain	4	5	4	4	3
Netherlands	4	4	4	4	4

• Score 5 – Full implementation, high maturity, and active interoperability with other EU systems.
• Score 4 – Advanced deployment with widespread use, but limited in certain areas.
• Score 3 – Moderate readiness, basic functionality available, but lacking full alignment.
• Score 2 – Partial implementation, low adoption, or missing interoperability components.
• Score 1 – Incipient or absent implementation of the evaluated capability.

This table presents the scores assigned to EU member states across the five dimensions relevant to eIDAS 2.0 readiness defined earlier. The scores were assigned on a 1-to-5 scale based on publicly available technical reports, ENISA incident disclosures, and national trust service provider registries. Evaluation criteria include the organizational model for digital identity governance, level of mobile ID adoption, QTSP ecosystem diversity, implementation of eIDAS node and metadata interoperability, and active participation in EBSI or EU wallet pilots. The scores represent increasing levels of maturity and alignment with eIDAS 2.0 objectives, ranging from incipient or absent implementation (1) to full deployment with active cross-border interoperability (5). Intermediate scores reflect varying degrees of readiness, functionality, and integration, as detailed in the accompanying legend.

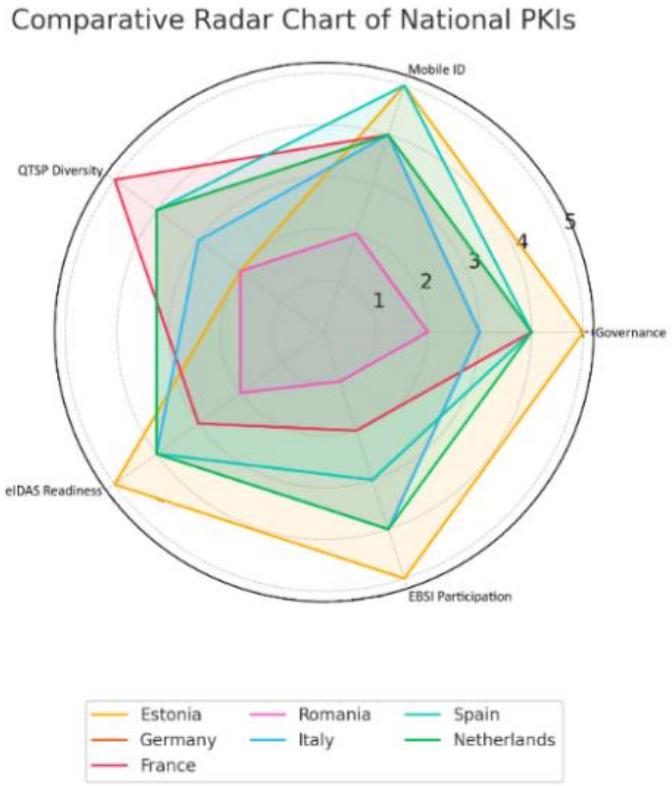

Fig. 2: Heatmap of PKI Readiness by Country.

The radar chart illustrates the relative strengths and weaknesses of each national PKI ecosystem. Estonia exhibits a consistently high maturity profile, with top scores in Mobile ID, eIDAS node readiness, and EBSI participation. Germany and the Netherlands also demonstrate robust performance, though slightly behind in QTSP diversity and EBSI engagement. France leads in QTSP diversity but shows weaker alignment in interoperability and EU infrastructure adoption. Italy and Spain score moderately across most dimensions, particularly in Mobile ID, but reveal gaps in standardization. Romania registers the lowest scores overall, reflecting early-stage infrastructure, limited user adoption, and slow alignment with EU frameworks.

3. PKI Maturity Levels Across Member States

Based on the Digital Identity Maturity Index and complementary readiness indicators, the seven countries fall into three general categories of PKI maturity: **high**, **moderate**, and **low**. Each group reflects the balance between infrastructure robustness, governance models, and user adoption levels.

Table 2

PKI Maturity Overview by Country.

Country	Governance Model	Mobile ID	QTSP Model	eIDAS Node	EBSI Participation	DIMI Score
Estonia	Centralized	High	Public	Full	Active	4.8
Germany	Federated	Medium	Mixed	Full	In Progress	4.3
France	Mixed	Medium	Private	Partial	Early Stage	3.9
Romania	Centralized	Low	Public	Ongoing	Limited	2.4
Italy	Mixed	High	Mixed	Full	Active	4.1
Spain	Mixed	High	Private	Full	Pilot Phase	4.0
Netherlands	Mixed	High	Mixed	Full	Pilot Phase	4.2

Table 2 provides a comparative overview of the evaluated countries across six key dimensions that influence digital identity maturity under eIDAS 2.0. These include the governance structure of national identity systems, the level of mobile ID adoption, the diversity and control model of Qualified Trust Service Providers (QTSPs), the status of eIDAS node deployment, and engagement in the European Blockchain Services Infrastructure (EBSI). The final column reflects the composite DIMI Score, used as a maturity indicator throughout this study.

At the foundation of any robust PKI lies the ability to associate cryptographic credentials with verifiable, legally recognized digital identities. In the context of eIDAS 2.0, this requires seamless integration between national identity systems and Qualified Trust Service Providers that issue electronic certificates for authentication, signing, and sealing.

A coherent PKI architecture connects three critical layers:

- Identity assurance (via a national digital identity system),
- Credential issuance (via QTSPs),
- Cross-border interoperability (via eIDAS Nodes and metadata compliance).

In Estonia, for example, these elements are tightly integrated: the national ID system feeds directly into Smart-ID and is managed by a central trust provider. Germany follows a more modular, federated model. In contrast, Romania is currently developing its central digital identity platform, ROeID, which is designed to unify citizen identity access across public services. While promising, ROeID remains in early implementation and is not yet fully integrated with QTSP services or eIDAS technical frameworks.

This gap limits Romania's ability to issue fully qualified certificates linked to national identity, and to validate them across borders. As such, its PKI ecosystem remains incomplete when benchmarked against the eIDAS 2.0 reference architecture.

Hölbl et al. identified key weaknesses in eIDAS nodes—including organizational independence, remote video identification, and technical heterogeneity—that must be addressed in the upcoming eIDAS 2.0 framework [22, p. 10].

High Maturity Countries

Estonia, Germany, and the Netherlands show advanced preparedness for eIDAS 2.0. Estonia leads with a centralized model, full mobile ID penetration, and seamless EBSI integration through Smart-ID [11]. Germany leverages a federated structure with modular QTSPs and strong node performance, supported by platforms like Governikus [8]. The Netherlands, with its mixed model, stands out for wallet interoperability via IRMA [10], and early implementation of decentralized identity credentials.

Moderate Maturity Countries

Italy, Spain, and France demonstrate solid infrastructure but face challenges in coordination and integration. Italy operates both SPID and CIE systems under a mixed governance model. Spain emphasizes mobile identity and private QTSPs via Cl@ve, while France relies heavily on private QTSPs with slower eIDAS node deployment.

Low Maturity Country

Romania remains in the early stages of digital identity adoption. Despite a centralized policy and the ROeID platform, it shows limited user uptake, partial eIDAS node readiness, and minimal blockchain participation.

4. Key Readiness Factors for PKI and Digital Identity Adoption

The following sections unpack the logic behind the scoring dimensions already introduced, offering the analytical rationale that supports the maturity classification presented in Section 3.

Beyond technical infrastructure, national readiness for eIDAS 2.0 depends on structural, organizational, and policy-related elements. This section expands on the key dimensions that underlie the Digital Identity Maturity Index introduced earlier. While comparative scores have been presented, a detailed understanding of each readiness factor is essential to interpret national differences and identify priority areas for policy reform.

4.1 Governance Models and Institutional History

The structure of digital identity systems often reflects a country's broader administrative culture. Estonia represents a centralized approach where one public infrastructure supports all major trust services. Its success is linked to post-independence reforms and digital literacy campaigns.

Germany, by contrast, follows a federated model due to its constitutional framework. Different federal entities oversee various QTSPs, contributing to diversity but requiring more coordination.

Hybrid models are seen in France, Spain, Italy, and the Netherlands. These countries combine government regulation with private-sector QTSPs. Romania also uses a centralized model but lacks Estonia's user outreach and interoperability mechanisms.

4.2 QTSP Ownership: Public vs. Private Provisioning

The ownership of Qualified Trust Service Providers affects innovation, compliance, and flexibility. Countries with public QTSPs (e.g., Estonia and Romania) often have more direct control but limited-service diversity.

In contrast, France and Spain rely heavily on private QTSPs, which can innovate faster but sometimes lack uniform compliance. In France, ANSSI oversees both hierarchical and private-sector PKIs, with over 28 qualified CAs under eIDAS—demonstrating a hybrid public–private trust model [25, pp. 4–5]. The Netherlands combines public oversight with non-profit and commercial providers, offering a balanced approach.

4.3 Semantic Interoperability and Metadata Alignment

Even with compatible certificate formats, semantic differences can block interoperability. Member states differ in how they define certificate lifetimes, revocation policies, and assurance levels. These variations complicate cross-border validation [12]. Sharif et al. analyze 24 notified national eID schemes and emphasize the trend towards decentralized and privacy-preserving identity architectures under eIDAS 2.0 [23, pp. 5–7].

Standardization efforts led by ETSI [12] and ENISA [2] focus on:

ETSI [12] EN 319 412 (certificate profiles), TS 119 312 (validation policy), TS 119 511 (qualified signature creation devices).

Germany and the Netherlands are already aligned with these standards. Estonia uses automated certificate validation through Smart-ID [11] and X-Road. Romania and Italy are in the process of updating legacy schemas.

According to OECD, national digital identity governance is shaped by constitutional and administrative traditions, which can explain why Germany uses a federated approach while Estonia retains a centralized architecture [21, p. 9].

4.4 Transparency and KPI Monitoring

Tracking digital identity adoption and trust service usage is essential for policy development. Estonia publishes regular Smart-ID [11] usage data. Germany maintains transparency dashboards. The Netherlands and Spain provide metrics on authentication transactions.

However, Romania, France, and Italy lack consistent public reporting. This makes it harder to evaluate progress or compare systems effectively. A common

KPI framework—such as the Digital Identity Maturity Index—can support cross-country benchmarking. (see Table 1).

The World Bank's ID4D 2021 report notes that over 850 million people lack verifiable digital identity, and even within the EU, public reporting on digital ID use remains inconsistent [19, p. xii].

5. Technical Infrastructure and Cryptographic Readiness

A secure and resilient PKI system relies on well-designed technical foundations. This section evaluates four essential components: how certificates are issued and validated, the strength and compliance of cryptographic standards, readiness for post-quantum cryptography (PQC), and the use of hardware security modules (HSMs) to protect trust anchors.

5.1 Certificate Lifecycle Management

Countries differ in how they manage the lifecycle of digital certificates, particularly in issuing, validating, and revoking them.

Estonia automates this process entirely, using Online Certificate Status Protocol (OCSP) responders integrated into its Smart-ID [11] system. Germany employs a modular architecture across its federated QTSPs, supporting both OCSP and Certificate Revocation Lists (CRLs). France relies on private QTSPs, where EJBCA [9]-based systems mainly use CRLs with limited OCSP functionality. Romania still uses a largely manual process, with basic CRL-based revocation. Italy and Spain enable OCSP through card-based systems (CIE and DNIe), though with varying consistency across providers. The Netherlands uses OCSP and CRLs in its IRMA [10]-based identity wallet, aligning with modern identity frameworks.

A systematic literature review reveals that trust-models such as Bridge CAs and Cross-Certification face major scalability and liability limitations in large-scale PKI implementations [24, pp. 12–14].

5.2 Cryptographic Standards and Interoperability

All countries meet the minimum requirements of the eIDAS Regulation [1], including RSA 2048-bit key sizes and SHA-2 hashing.

Some countries have moved ahead with more modern algorithms:

- Estonia and Germany are transitioning to elliptic curve cryptography (ECC), using algorithms such as Brainpool and ECDSA.
- The Netherlands also supports ECC within its decentralized identity solutions.

Standardizing certificate formats and cryptographic parameters is essential for cross-border trust. Most implementations follow ETSI [12] EN 319 and TS 119

series standards, ensuring compatibility for validation across different national systems.

5.3 Post-Quantum Cryptography Readiness

None of the countries evaluated has implemented quantum-resistant cryptography in production environments. However, testbeds and feasibility studies are underway:

- Germany and Estonia have started hybrid certificate pilots that combine traditional and PQC algorithms.
- France and Romania have draft plans for transition but no live deployments.
- Spain, Italy, and the Netherlands are monitoring developments but remain in the exploratory phase.

The absence of clear national road maps for PQC adoption remains a concern, especially given recommendations in cybersecurity reports from ENISA and national agencies. Public benchmarks, audit trails, and performance data are needed to support PQC readiness.

ENISA's 2021 analysis emphasizes that hybrid certificates—combining classical and PQC algorithms—should be prioritized in critical infrastructure to enable secure migration paths [17, p. 27].

NIST's selection of CRYSTALS-Kyber and CRYSTALS-Dilithium as standard algorithms reflects the urgency of adopting PQC-compatible protocols across EU trust services [18, p. 3].

5.4 Hardware Security Modules (HSMs)

HSMs provide tamper-resistant environments for key generation, storage, and digital signature creation. Their use varies by country:

- Estonia, Germany, and the Netherlands use certified HSMs extensively across public and private QTSPs.
- Romania is in early stages, with centralized infrastructure under development.
- Italy and Spain use HSMs mainly in specific sectors (e.g., card issuance authorities) but lack a unified national approach.
- France exhibits fragmented use, depending on individual private QTSP implementations.

6. Cybersecurity and Trustworthiness of National PKI Systems

Although national PKI systems serve as foundational trust anchors under eIDAS, they remain exposed to recurring cybersecurity risks such as certificate mis issuance, delayed revocation, and weak key lifecycle management. Documented incidents in France, Germany, and Spain have highlighted compliance lapses ranging from compromised certificate revocation delays to phishing campaigns targeting identity portals. These examples illustrate the need for uniform operational standards across both public and private QTSPs.

According to ENISA's 2022 analysis [17, p. 5], frequent issues include misconfigured trust service software, slow incident response, and inadequate transparency in revocation practices. ENISA recommends enhancing audit capabilities and publishing standardized security metrics to rebuild trust and ensure real-time accountability. At the national level, CSIRTs such as CCN-CERT (Spain), CSIRT.RO (Romania), and BSI-CSIRT (Germany) contribute to risk monitoring and incident reporting, while Estonia and the Netherlands stand out for maintaining regular audit logs and public compliance disclosures.

To meet the evolving demands of eIDAS 2.0, national PKI ecosystems must integrate cybersecurity best practices, align with ENISA guidance, and support verifiable incident response frameworks that foster both public and cross-border trust.

7. Strategic Outlook for eIDAS 2.0 Implementation

The implementation of eIDAS 2.0 and the European Digital Identity Wallet represents a transformative step in harmonizing digital trust services across the EU [13]. Member states are advancing at varying paces, influenced by their existing infrastructure, technical alignment, and openness to self-sovereign identity (SSI) models. Estonia leads in wallet readiness, having already deployed Smart-ID for public services and EBSI use cases. Germany and the Netherlands follow closely, piloting advanced wallet platforms for academic and municipal credentials. Italy and Spain are testing wallet functions in specific domains but must navigate dual identity systems (e.g., SPID, DNIe, Cl@ve), while France and Romania remain in early deployment phases, still finalizing foundational infrastructure.

Countries with well-aligned technical stacks—particularly Estonia, Germany, and the Netherlands—benefit from conformance to ETSI metadata standards and existing support for eIDAS-compatible APIs and certificates. These enable smoother wallet rollout and eventually SSI extension. The Netherlands, through IRMA, has pioneered privacy-preserving attribute sharing, while Germany explores decentralized identifiers (DIDs) and verifiable credentials in regulated sectors. Estonia's X-Road interoperability layer facilitates selective disclosure and attribute-based authentication. However, SSI frameworks in France, Spain, Italy,

and Romania are still in exploratory stages, lacking formal policy tracks or integration with Qualified Trust Service Provider (QTSP) regimes [12].

To support broad adoption and interoperability, member states should align wallet APIs with national eID systems, adopt standardized metadata per ETSI EN 319/TS 119, and publish clear SSI governance frameworks. A coordinated EU sandbox for wallet and SSI testing—complemented by multilingual user interfaces and post-quantum cryptography (PQC) readiness—will be essential to ensure eIDAS 2.0 delivers both technical robustness and citizen trust [12].

7.1 Estimation of Digital Identity Adoption in Romania

Recent national reports indicate that Romania's digital identity ecosystem is still in an early adoption phase but is expected to expand rapidly with the operationalization of the ROeID platform. According to the *Ministry of Research, Innovation and Digitalization (MCID, 2025)* [26] and the *Digital Economy and Society Index (DESI 2024)* [27], approximately **6–8 % of Romanian citizens** currently possess a qualified digital certificate that can be used for electronic signature, corresponding to roughly **1.5 million active digital identities**.

The introduction of mobile-based identity mechanisms under ROeID and their planned integration with **Ghișeul.ro**, **SPV (Virtual Private Space)**, and commercial banking applications are projected to accelerate uptake. Conservative forecasts suggest that mobile identity usage could reach **30 % of the adult population by 2027** and **55–60 % by 2030**, assuming continued government support and alignment with eIDAS 2.0 wallet standards.

Based on these adoption trajectories, Romania's **Digital Identity Maturity Index (DIMI)**—which currently stands at **2.4 (2025)**—is expected to increase to **3.5 by 2027** and to approach **4.0 by 2030**, aligning it with the current EU average. These projections assume a compound annual growth rate of approximately **25 %** in digital ID issuance, like trends observed among late-adopter member states in DESI data.

Table 3

Projected Evolution of Digital Identity Adoption in Romania.

Year	Citizens with Active Digital ID	Mobile ID Penetration	Projected DIMI
2025	6–8 % (≈ 1.5 million users)	< 5 %	2.4
2027	≈ 30 % (≈ 5.5 million users)	≈ 25 %	3.5
2030	≈ 55–60 % (≈ 10 million users)	≈ 45–50 %	4.0

These estimates suggest that Romania could move from a **low-maturity** to a **moderate-maturity** status within five years, provided that the national ROeID system achieves interoperability with QTSP infrastructures and maintains transparent KPI monitoring. Continued alignment with ETSI EN 319 and TS 119

standards and participation in EBSI pilots will remain essential to sustain this adoption trajectory under eIDAS 2.0.

8. Conclusions and Recommendations

This cross-country comparative analysis shows substantial progress in digital identity infrastructure and trust service deployment across seven EU member states [12]. Yet, eIDAS 2.0 readiness remains fragmented due to variations in governance models, citizen adoption rates, technical alignment with ETSI standards, and the degree of engagement with emerging initiatives such as digital wallets and EBSI. Centralized models like Estonia's enable coherent policy implementation, while federated and hybrid systems such as those in Germany and the Netherlands offer flexibility but require tighter coordination to achieve semantic and cryptographic interoperability.

Strategic gaps persist in areas such as post-quantum cryptography (PQC), which is still in pilot phases, and self-sovereign identity (SSI), which is evolving outside the formal regulatory scope. To accelerate convergence, countries must harmonize national certificate profiles and trust metadata with ETSI EN 319 and TS 119 standards, launch digital wallet APIs integrated into national eID systems, and conduct PQC pilots that include transparent benchmarking and audit trails. Short-term priorities also include expanding EBSI use cases, standardizing multilingual wallet UX, and validating interoperability through shared testbeds [12].

Looking ahead, EU member states should establish SSI policy tracks to address certification and cross-border recognition, build real-time monitoring dashboards for digital ID performance and trust service incidents, and embed GDPR safeguards into AI-based identity verification. These steps are essential to ensure that eIDAS 2.0 delivers on its vision of a secure, user-centric, and interoperable European digital identity ecosystem.

REFERENCES

[1] European Commission, "eIDAS 2.0 Proposal and Framework," 2023. [Online]. Available: https://digital-strategy.ec.europa.eu

[2] European Union Agency for Cybersecurity (ENISA), Trust Services and Cybersecurity Trends, 2022. [Online]. Available: https://www.enisa.europa.eu

[3] EU Trusted List Browser, "QTSP Accreditation Records," 2023. [Online]. Available: https://eidas.ec.europa.eu/efda/home

[4] BSI, Germany Federal Office for Information Security: Annual Report, 2022. [Online]. Available: https://www.bsi.bund.de

[5] ANSSI, Agence nationale de la sécurité des systèmes d'information: Annual Activity Report, 2022. [Online]. Available: https://www.ssi.gouv.fr

[6] CCN-CERT, Spain Cybersecurity Incident Reports, 2022. [Online]. Available: https://www.ccn-cert.cni.es

[7] CSIRT Romania, Public Security Disclosures, 2023. [Online]. Available: https://www.cert.ro

[8] Governikus GmbH & Co. KG, Secure Digital Identity Services Overview, 2022. [Online]. Available: https://www.governikus.de

[9] PrimeKey Solutions, EJBCA Enterprise PKI Documentation, 2022. [Online]. Available: https://www.ejbca.org

[10] IRMA Project, "Privacy by Design Foundation: IRMA Overview," 2023. [Online]. Available: https://privacybydesign.foundation/irma-en/

[11] SK ID Solutions, Smart-ID Usage Statistics, 2023. [Online]. Available: https://www.skidsolutions.eu

[12] ETSI, EN 319 and TS 119 Series Standards for Trust Services, 2022. [Online]. Available: https://www.etsi.org

[13] Digital Identity Wallet Consortium, "Pilot Use Cases and Interoperability Roadmaps," 2023. [Online]. Available: https://digital-identity-wallet.eu

[14] Global LEI Foundation, "Trusted Identity Integration Reports," 2023. [Online]. Available: https://www.gleif.org

[15] CEF Digital, "eDelivery Conformance Testing Tools," 2023. [Online]. Available: https://ec.europa.eu/cefdigital

[16] European Commission, "Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity," COM/2021/281 final. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[17] European Union Agency for Cybersecurity (ENISA), Post-Quantum Cryptography: Current State and Quantum Mitigation, May 2021, pp. 1–35. Available: https://www.enisa.europa.eu/publications

[18] NIST, Post-Quantum Cryptography Standardization: Finalist Algorithms, 2024, pp. 3–7. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[19] World Bank, ID4D Global Dataset 2021: Global Identification Systems Analysis, World Bank Group, 2021, pp. xii–18. Available: https://id4d.worldbank.org

[20] Bavdekar, S., Patel, S., & Gupta, A., Post Quantum Cryptography: Techniques and Implementation Considerations, arXiv preprint arXiv:2210.14578, 2022. Available: https://arxiv.org/abs/2210.14578

[21] OECD, Digital Identity Management: Enabling Innovation and Trust in the Digital Economy, OECD Publishing, 2022, pp. 8–20. Available: https://www.oecd.org/sti/digital/identity.htm

[22] M. Hölbl, B. Kežmah, and M. Kompara, "eIDAS Interoperability and Cross-Border Compliance Issues," Mathematics, vol. 11, no. 2, pp. 1–24, 2023.

[23] *A. Sharif, M. Ranzi, R. Carbone, G. Sciarretta, F.A. Marino, and S. Ranise,* "The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes," Applied Sciences, vol. 12, no. 24, art. 12679, Dec. 2022.

[24] [Author(s)], "Analysis of Trust Models in Public Key Infrastructure: A Systematic Literature Review of Interoperability Challenges," MJoSHT, vol. 11, no. 1, pp. 95–110, 2025.

[25] World Bank, "Public key infrastructure: France as well as eIDAS for cross-border interoperability within the EU," P178616, 2023, pp. 1–8.

[26] Ministry of Research, Innovation and Digitalization (MCID), *Romanian Digital Identity and ROeID Implementation Strategy 2025–2030*, Bucharest, 2025. [Online]. Available: https://www.mcid.gov.ro

[27] European Commission, *Digital Economy and Society Index 2024: Country Report – Romania*, Luxembourg: Publications Office of the European Union, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu

Appendix: Key Acronyms and Terms

ANSSI – Agence nationale de la sécurité des systèmes d'information (France)

BSI-CSIRT – BSI's Computer Security Incident Response Team

CCN-CERT – Centro Criptológico Nacional – CSIRT (Spain)

CIE – Carta d'Identità Elettronica (Italy)

Cl@ve – Spain's federated login platform

CSIRT – Computer Security Incident Response Team

DIMI – Digital Identity Maturity Index: Composite metric evaluating identity coverage, e-signature use, and QTSP availability.

DNIe – Documento Nacional de Identidad electrónico (Spain)

EBSI – European Blockchain Services Infrastructure: EU-led platform for decentralized digital credentials

eIDAS – EU Regulation on electronic Identification, Authentication and Trust Services

Governikus – Governikus GmbH & Co. KG – German provider of secure digital identity services

HSM – Hardware Security Module: A physical device that protects and manages digital keys

IRMA – "I Reveal My Attributes" (NL SSI initiative)

OCSP / CRL – Protocols for certificate revocation status checks: Online Certificate Status Protocol / Certificate Revocation List

PKI – Public Key Infrastructure: A system of digital certificates, CAs, and related infrastructure used to secure electronic communications.

QTSP – Qualified Trust Service Provider: An entity legally authorized under eIDAS to issue trust services (e.g., digital certificates)

SPID – Sistema Pubblico di Identità Digitale (Italy)

SSI – Self-Sovereign Identity: A model allowing users to control and share identity credentials without relying on centralized issuers.