BEYOND DC4EU

Advancing European Digital Identity through Trust Frameworks, Education and Social Security Pilots

Alex Grech and Klaudia G. Farkas January 2026 3CL Foundation

About this Document

The DC4EU Strategic Committee commissioned this report to translate pilot findings into policy recommendations for European Digital Identity Wallet deployment. The authors, serving on the Strategic Committee, coordinated a Scientific Committee analysing critical technical and policy challenges, and the Committee's publications appear in the Further Readings section.

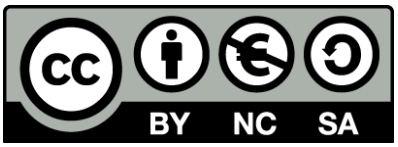
This analysis synthesises multiple evidence sources: Scientific Committee research outputs, over two years of market intelligence from DC4EU working group participation, weekly Strategic Committee discussions, and systematic analysis of opportunities and barriers documented through institutional surveys, technical testing, and direct observation across 101 institutions in twenty-five countries.

The authors sought validation from Strategic Committee members, Scientific Committee contributors, and implementation leads. The urgent publication timeline (informing Q1 2026 policy decisions) constrained full validation. Policy recommendations (Sections 5-8) represent informed analysis based on empirical evidence.

We are particularly grateful for the contributions of the following members of the DC4EU Strategic Committee for reviewing the document and providing insights that are reflected in this published version: Ignacio Alamillo-Domingo, Lluis Ariño-Martin, Gerd Bauer, Teemu Kääriäinen, Eugene McKenna and Klaas Wierenga.

Published January 2026 by the 3CL Foundation, Malta.

ISBN 978-9918-0-1495-8



This publication is licensed under the Creative Commons Attribution NonCommercial ShareAlike 4.0 Unported (CC BY-NC-SA EU 4.0)

Credits Cover Illustration: Google Gemini AI / Nano Banana. Layout & Text: 3CL Foundation.

Citation: Grech, A. and Farkas, K.G. (2026). *Beyond DC4EU. Advancing European Digital Identity through Trust Frameworks, Education and Social Security Pilots*. 3CL Foundation. Downloadable from www.3CL.org/resources

Contents

About this Document 1
Tables 4
Acronyms 5
Glossary 7
Executive Summary 12
1 Scope: The Critical Window for Execution 17
2 Background: The EUDIW Paradigm 19
2.1 The Legal Foundation: eIDAS 2.0 and GDPR 20
2.1.1 Governance Roles: Commission vs. Member States in EAA/QEAA 22
2.2 Core Features of the EUDIW and User Sovereignty 23
2.3 The Strategic Context: Architecture Reference Framework (ARF) 24
3 Operational Success: The Pluralistic Coexistence Blueprint 28
3.1 European Blockchain Services Infrastructure (EBSI) 30
3.2 OpenID Protocols for Interoperability 32
3.3 The Pluralistic Trust Model: EBSI, OpenID and PKI 34
3.3.1 Foundational Legal Basis and PKI 34
3.3.2 The Pluralistic Trust Component Summary 35
3.4 Key Technical Achievements 37
4 Key Pilot Domains 39
4.1 The Education Domain and Professional Qualifications: Piloting Digital Academic Credentials 40
4.1.1 Core Pilot Success and Technical Viability 41
4.1.2 The Trust Integration Model: Bridging Academic Identity (eduGAIN) 45
4.2 The Social Security Domain: EHIC and PDA1 49
4.2.1 Implementation and Workflow 51
4.3 Architectural Proof: The Hybrid Trust Model in Practice 59
5 Systematic Barriers & Challenges 65
5.1 Legal Foundations & Regulatory Fragmentation 65
5.2 Technical & Interoperability and ARF gaps 67
5.3 Governance & Operational Fragmentation 69
5.4 Funding & Resources 70
5.5 User Experience & Trust 72
6 Recommendation: From Technical Blueprint to Political Execution 74

6.1 Legal Clarity and Policy Harmonisation 75
6.2 Harmonised Governance 76
6.3 Sustainable Funding and Institutional Capacity 78
6.4 Architectural Interoperability 79
6.5 Citizen Trust and User Experience 80
7 Metrics of Success: Key Performance Indicators for the 2026 Mandate 82
7.1 Quantitative Impact and Adoption Targets 82
7.2 Qualitative Alignment with Policy Pillars 83
7.3 Monitoring and Accountability Framework 86
8 Roadmap / Action Plan Outline 87
9 Conclusion 93
Further Reading 96

Tables

Table 1: European Commission vs Member State Governance Roles 22
Table 2: The Three Trust Components of the Pluralistic Architecture 35
Table 3: Contrasting Institutional Environments 39
Table 4: Cross-Border Recognition Performance Metrics 43
Table 5: Social Security Credentials 49
Table 6: Request and Identity Binding Comparison 52
Table 7: Point of Use Presentation Comparison 53
Table 8: The Complete Transaction Timeline - Three Trust Layers Working Together 62
Table 9: Legal Fragmentation Manifestations 66
Table 10: Technical and Interoperability Barriers 68
Table 11: Governance Fragmentation Dimensions 70
Table 12: Funding Model Comparison 71
Table 13: User Experience Failure Patterns 73
Table 14: Action Pillars Overview 74
Table 15: Legal Clarity Implementation Timeline 76
Table 16: Governance Board Functions 77
Table 17: Funding Model Transformation 78
Table 18: Integration Cost Reduction 79
Table 19: User Experience Requirements 80
Table 20: Quantitative Performance Indicators 82
Table 21: Qualitative Alignment Milestones 84
Table 22: Phase 1 - Foundation and Governance 87
Table 23: Phase 2 - Technical Integration and Policy Finalisation 88
Table 24: Phase 3 - Scale-up and Deployment 89
Table 25: Phase 4 - Sustainability and Innovation 90

Acronyms

This document uses numerous technical and regulatory acronyms. All acronyms are defined on first use within each major section.

API: Application Programming Interface

ARF: Architecture Reference Framework

CA: Certificate Authority

CIR: Commission Implementing Regulation

DC4EU: Digital Credentials for Europe

DG CNECT: Directorate-General for Communications Networks, Content and Technology, European Commission

DID: Decentralised Identifier

DP: Data Provider

EAAs: Electronic Attestations of Attributes

EBSI: European Blockchain Services Infrastructure

EC: European Commission

EDC: European Digital Credentials

EDICG: European Digital Identity Cooperation Group

eduGAIN: Global federated identity service

EHIC: European Health Insurance Card

eIDAS: electronic IDentification, Authentication and trust Services

ELA: European Labour Authority

ELM: European Learning Model

ENISA: European Union Agency for Cybersecurity

ESIP: European Social Insurance Platform

ETSI: European Telecommunications Standards Institute

EUDIW: European Digital Identity Wallet

EUDI: European Union Digital Identity

EWP: Erasmus Without Paper

FIM: Federated Identity Management

GDPR: General Data Protection Regulation

HEI: Higher Education Institution

IAs: Implementing Acts

IdP: Identity Provider

JSON: JavaScript Object Notation

JSON-LD: JSON for Linked Data

JWT: JSON Web Tokens

LoA: Levels of Assurance

LSP: Large-Scale Pilots

OIDC: OpenID Connect

OIDC4VCI: OpenID for Verifiable Credential Issuance

OIDC4VP: OpenID for Verifiable Presentation

PDA1: Portable Document A1

PID: Personal Identification Data

PKI: Public Key Infrastructure

PuB-EAAs: Public Body Electronic Attestations of Attributes

QEAAs: Qualified Electronic Attestations of Attributes

QES: Qualified Electronic Signatures

QSeal: Qualified Electronic Seals

QTSP: Qualified Trust Service Provider

RFC: Request for Comments

RI: Reference Implementation

RP: Relying Party

SDG: Single Digital Gateway

SD-JWT: Selective Disclosure for JSON Web Tokens

SDK: Software Development Kit

SDP: Selective Disclosure Policy

SP: Service Provider

SSI: Self-Sovereign Identity

SSO: Single Sign-On

TL: Trusted List

TSP: Trust Service Provider

UX: User Experience

VC: Verifiable Credentials

VP: Verifiable Presentation

VDR: Verification Data Registry

W3C: World Wide Web Consortium

W3C-VCDM: W3C Verifiable Credentials Data Model

WG: Working Group

ZKPs: Zero-Knowledge Proofs

Glossary

Application Programming Interface (API) - A set of defined rules for software interaction, primarily used in the EUDI Wallet ecosystem for standardised communication (e.g., OIDC4VCI/OIDC4VP) between Wallets, Issuers, and Relying Parties.

Architecture and Reference Framework (ARF) - The comprehensive technical and organizational standard established by the European Commission that specifies how EUDI Wallets connect and communicate, defines credential formats, and sets security and interoperability requirements.

Certificate Authority (CA) - An entity in traditional Public Key Infrastructure (PKI) that issues digital certificates. The EUDI Wallet ecosystem relies on CAs to establish trust, as the root certificates (Trust Anchors-technically referred to as Service Digital Identifiers in the ETSI Trusted List standard) of key ecosystem actors are verified and published within the national Trusted Lists required by the eIDAS Regulation.

Commission Implementing Regulation (CIR) - Legal rules created by the European Commission that specify the technical and operational details for how eIDAS 2.0 services and EUDI Wallets must function in practice (e.g., core wallet functions, technical protocols).

Digital Credentials for Europe (DC4EU) - The European Union-funded large-scale pilot project that tests real-world applications of digital credentials in the education and social security sectors using the EUDI Wallet and its underlying trust frameworks.

Decentralised Identifier (DID) - A unique, cryptographically verifiable identifier used in Self-Sovereign Identity (SSI) systems, particularly those leveraging the W3C Verifiable Credentials Data Model and Verifiable Data Registries.

Electronic Attestation of Attributes (EAA) - The generic term for any digital proof of an attribute (e.g., diploma, driving license, age, profession) issued by an authorised entity for storage and sharing via the EUDI Wallet.

European Blockchain Services Infrastructure (EBSI) - A pan-European infrastructure acting as a Trusted Ledger that provides a network of Verification Data Registries (VDRs) for managing governance information, key revocation, and ensuring the authenticity of credentials, compliant with the eIDAS 2.0 trust framework.

European Digital Credentials (EDC) - Standardised digital credentials used in DC4EU's framework for education and professional qualification attestations, fully compliant with W3C Verifiable Credentials standards.

European Digital Identity Cooperation Group (EDICG) - The governance body, successor to the eIDAS Expert Group, that facilitates collaboration between EU Member States and the European Commission on digital identity matters and develops common tools for the framework.

eduGAIN - The inter-federation service that connects existing national identity federations in the Research and Education sector, allowing users to access resources across Europe. It is a key legacy trust system being integrated with the EUDI Wallet.

European Health Insurance Card (EHIC) - A physical card granting EU citizens access to medical treatment in other Member States, which is a core PuB-EAA pilot use case within the DC4EU social security domain.

electronic IDentification, Authentication and trust Services (eIDAS) - The original EU Regulation (No 910/2014) that created a legal framework for electronic identification and digital trust services across the European Union.

electronic IDentification, Authentication and trust Services Amended eIDAS Regulation (eIDAS2) - The updated Regulation (EU) 2024/1183, which amends the existing eIDAS Regulation (Regulation

(EU) 910/2014), legally establishes the EUDI Wallet, defines requirements for Qualified and Public Body Electronic Attestations of Attributes (QEAA/PuB-EAA), and mandates their cross-border recognition.

European Health Data Space (EHDS) - The European Health Data Space is a proposed, decentralized, and interoperable European framework for the secure exchange of health data across the EU. Its dual purpose is to empower citizens with direct access to their electronic health records for Primary Use (improving cross-border healthcare) and to provide secure access to pseudonymised data for Secondary Use (accelerating research, innovation, and policymaking). The EHDS legal framework mandates high-assurance digital identity and authentication for access points, directly driving the implementation of solutions like the EUDI Wallet for both patient access and the verification of professional attributes (e.g., medical qualifications via EAAs).

European Learning Model (ELM) - A standard framework used by DC4EU to standardise educational attestations, ensuring that academic credentials are consistently understood and verified across different systems.

European Union Agency for Cybersecurity (ENISA) - The EU agency responsible for developing specialised cybersecurity certification schemes for EUDI Wallets to ensure they meet mandatory security and functionality standards.

European Social Insurance Platform (ESIP) - An association representing Social Security institutions across Europe, relevant to the social security pilot as a body that promotes comprehensive approaches to social security systems.

European Telecommunications Standards Institute (ETSI) - A standards organization that develops technical specifications for EUDI Wallets and Trust Service Providers (TSPs) that are crucial for compliance with the legal framework.

European Union Digital Identity (EUDI) - The comprehensive vision and ecosystem that enables citizens to securely prove their identity, share personal information, and access public and private services across national borders.

European Digital Identity Wallet (EUDI Wallet) - A digital application mandated by the revised eIDAS regulation that allows EU citizens to securely verify their identity, hold digital credentials, and choose what information to share while prioritizing privacy.

European Harmonisation Layer - An architectural recommendation for a central component or layer mandated to standardise metadata and schemas, easing the technical integration of diverse national IT systems with the EUDI Wallet ecosystem.

General Data Protection Regulation (GDPR) - The EU regulation that governs how personal data is processed. It is the legal basis for the EUDI Wallet's core design principles, such as Privacy by Design and data minimization (e.g., Selective Disclosure).

Implementing Acts (IA) - Legal instruments that establish core functionalities, certification requirements, and technical specifications for EUDI Wallets and trust services, adopted by the European Commission following eIDAS2.

Identity Provider (IdP) - In traditional authentication systems (e.g., eduGAIN), a trusted external organization that verifies a user's identity. The EUDI Wallet model shifts this control to the user via Self-Sovereign Identity (SSI).

JavaScript Object Notation for Linked Data (JSON-LD) - A method of encoding linked data using the JSON format to create structured, interconnected information, which is a common format for W3C Verifiable Credentials.

Levels of Assurance (LoA) - The degree of confidence in a person's claimed identity. A "High" LoA requires rigorous verification and strong authentication, which is essential for sensitive or legally significant EUDI Wallet transactions.

Non-qualified Electronic Attestation of Attributes (Non-qualified EAA) - Issued by a trusted entity (often private or non-governmental, like a university) that is not a QTSP. This is an essential, pragmatic model for high-volume sectors (like Education). Cross-border value: Their use is largely based on contracts and risk management; they do not enjoy the same automatic legal effect as QEAA or the specific public law character of PuB-EAA.

OpenID Connect (OIDC) - A secure authentication and authorisation protocol that serves as the foundational standard for the EUDI Wallet's interaction protocols (OIDC4VCI and OIDC4VP).

OpenID for Verifiable Credential Issuance (OIDC4VCI) - The primary protocol that enables secure, dynamic interactions between EUDI Wallets and trusted credential Issuers for the creation and distribution of digital credentials.

OpenID for Verifiable Presentation (OIDC4VP) - A protocol used by Relying Parties (Verifiers) to request and verify a Verifiable Presentation (VP) from a Wallet Holder, supporting dynamic requests and selective information disclosure.

OpenID Federation (OPIF) - A technical protocol specification developed by the OpenID Foundation that defines a scalable mechanism for establishing and maintaining multi-lateral trust among a large number of independent digital entities (such as Wallet Providers, Attestation Issuers, and Relying Parties) essential for the pan-European deployment of the EUDI Wallet.

OpenID Foundation (OIDF) - The organization responsible for developing and maintaining the OpenID Connect and Federation specifications, which are essential protocols for the EUDI Wallet.

Once-Only Principle Technical System (OOTS) - A system implementing the Once-Only Principle, which eliminates redundant information requests and improves efficiency in public services by enabling trusted data exchange between Member States.

Portable Document A1 - A formal entitlement document (a type of PuB-EAA) issued by national social security institutions to certify an individual's social security coverage when working temporarily abroad. It is a core pilot use case in DC4EU.

Personal Identification Data (PID) - A category of data supported by EUDI Wallets that securely links each Public Body Electronic Attestation of Attributes (PuB-EAA) to the holder's identity to ensure high-level assurance.

Public Key Infrastructure (PKI) - A traditional cryptographic security framework using digital signatures and certificate chains to ensure authenticity. The EUDI Wallet model evolves PKI with components like VDRs and Trusted Lists.

Public Body Electronic Attestations of Attributes (PuB-EAA) -Issued directly by an Authentic Source (a public sector organization, e.g., a national ministry or social security agency). Validated in the Social Security pilot (EHIC/PDA1). Cross-border value: PuB-EAA expresses official data from a competent authority and carries high evidential weight. Its automatic mutual recognition and specific legal effect across borders depends mainly on relevant EU sectoral law and eIDAS articles 45/45f.

Qualified Electronic Attestations of Attributes (QEAA) - Issued by a Qualified Trust Service Provider (QTSP), which is strictly assessed and listed on the EU Trusted List, offering the strongest legal certainty under eIDAS 2.0. Cross-border value: QEAA has the strongest legal effect for attributes, with automatic mutual recognition across Member States for relevant public sector uses and a strong presumption of reliability.

Qualified Electronic Signatures (QES) - A type of electronic signature that must be used to sign QEAAs or PuB-EAAs based on qualified certificates and qualified electronic signature creation devices, ensuring strong legal enforceability.

Qualified Electronic Seals (QSeal) - A type of electronic seal that must be used to seal QEAAs or PuB-EAAs based on qualified certificates and qualified electronic seal creation devices, ensuring the authenticity and integrity of the issuing organization.

Qualified Trust Service Provider (QTSP) - A private or public organization authorised and audited to issue Qualified Electronic Attestations of Attributes (QEAA), subject to the highest level of regulatory compliance.

Reference Implementation (RI) - Template or model software components (e.g., EUDI Wallet RI) that Member States and developers can use as a foundation for developing their EUDI Wallet systems.

Relying Party (RP) - An organization or Verifier that requires verified identity claims or entitlements and validates the Verifiable Presentations made by EUDI Wallet holders.

Selective Disclosure for JSON Web Tokens (SD-JWT) - A cryptographic format enabling precise, user-controlled disclosure of specific credential attributes while promoting privacy and data minimization.

Single Digital Gateway (SDG) - EU Regulation 2018/1724 requiring digital access to essential public services across borders, often implementing the Once-Only Principle.

Selective Disclosure Policy (SDP) - Policies defining conditions for sharing specific attributes (including PID) with Relying Parties, ensuring only the **minimum necessary information is disclosed** for a given purpose, complying with GDPR.

Schema Catalogue - A standardised library of credential and data formats (schemas) designed to ensure consistent understanding and verification of credentials across different EUDI Wallet systems (e.g., for EDC/ELM).

Self-Sovereign Identity (SSI) - An identity management philosophy emphasizing user control over personal digital identity and data, which the EUDI Wallet is designed to embody.

Trust Service Provider (TSP) - Any organization that issues verified electronic attributes (such as diplomas, licenses, or legal authorisations). TSPs can be qualified (QTSP) or non-qualified.

Verifiable Credentials (VC) - Digital credentials stored in EUDI Wallets that can be presented directly to verifiers and validated offline using cryptographic signatures and published trust sources.

Verification Data Registry (VDR) - A cryptographic registry, such as those used in EBSI, that provides an unchangeable, auditable, and discoverable infrastructure for trust sources, significantly simplifying key and revocation management.

Verifiable Presentation (VP) - The cryptographic artifact (a signed message) by which a Wallet Holder demonstrates possession of one or more Verifiable Credentials (VCs) and selectively discloses attributes to a Relying Party (RP).

World Wide Web Consortium (W3C) - The international standards organization that defines web specifications, notably the W3C Verifiable Credentials Data Model (W3C-VCDM) which forms the technical foundation for EUDI credentials.

W3C Verifiable Credentials Data Model (W3C-VCDM) - The foundational technical standard for structuring digitally signed and verifiable attribute attestations used by the EUDI Wallet ecosystem.

Zero-Knowledge Proofs (ZKP) - Cryptographic methods enabling users to prove possession of certain information (e.g., being over 18) without revealing the complete data or unrelated attributes, supporting maximum data minimization and privacy.

Executive Summary

Europe's 2026 digital identity mandate is achievable - but only with immediate, decisive action.

The Digital Credentials for Europe (DC4EU) project confirmed that the European Digital Identity (EUDI) Wallet ecosystem is technically viable for secure, cross-border use in foundational public domains. Across 101 institutions in 25 countries, we successfully issued and verified high-assurance credentials - digital diplomas, European health insurance cards, and social security coordination documents - across borders. The technology is proven. The architecture is validated. The protocols function reliably under real-world conditions.

What prevents deployment at scale is not technology: it is fragmented governance, unsustainable funding, legal uncertainty across Member States, and insufficient coordination. This report, commissioned by the DC4EU Scientific Committee, translates over two years of pilot findings into actionable policy recommendations. The analysis draws on Scientific Committee research, market intelligence from working group participation, weekly Strategic Committee discussions, and systematic barrier analysis across participating institutions.

This report demonstrates that the European Digital Identity Wallet is technically viable for secure, cross-border use in foundational public-service domains. The transition from successful pilots to deployment for the public service domain at the European scale by 2026, however, will not occur organically. While DC4EU has validated the technical viability of digital credentials in public sectors, appropriate uptake now requires a concerted focus on private sector integration to prevent the Wallet from becoming a siloed government tool. Operational tools must be made immediately available to both public and private institutions, accompanied by strategic incentives, ranging from reduced administrative overhead to new service-triggering business cases, to encourage early onboarding by private service providers. It requires immediate and decisive political execution.

The European Commission must therefore launch a dedicated Deployment Funding Call to enable execution and institutionalisation. This action is required now—not in response to a future crisis of unpreparedness.

The Timeline Imperative

This report was published in January 2026 and addresses a critical window. Member States are subject to a legal obligation to deploy functional EUDI Wallets by December 2026. This leaves less than twelve months primarily for execution rather than for initial planning. While indicative timelines suggest that governance set-up, funding allocation, technical deployment, integration, testing, and citizen onboarding could be sequenced within this period, the margin for delay is limited.

A realistic transition period extending beyond 2026 - allowing for phased deployment, operational stabilisation, and gradual onboarding - would therefore be necessary to ensure effective and sustainable implementation across the public service domain at European scale.

The challenge is further shaped by existing capacity loss. DC4EU funding ended in July 2025. Survey data confirms that sixty percent of smaller public bodies report cannot sustain specialised capabilities beyond twelve to eighteen months without guaranteed multi-annual funding; thirty-five percent have already lost key technical staff. Prolonged uncertainty increases the risk of continued capacity erosion, as trained personnel seek alternative opportunities, institutional knowledge diminishes, and systems shift toward maintenance-only operation.

The Operational Success: Pluralistic Coexistence

DC4EU achieved cross-border issuance and verification of high-assurance Electronic Attestations of Attributes in two strategic domains: Education (digital diplomas, professional qualifications) and

Social Security (European Health Insurance Card, Portable Document A1). These domains represent opposite ends of the institutional spectrum: modern, federated education systems versus predominantly legacy-based, centrally administered social security systems at the national level. Success across both proves the architecture manages Europe's institutional diversity.

The critical architectural insight was the **Pluralistic Coexistence Strategy**. This was not a predetermined design choice, but an empirical finding emerging from implementation experience. It demonstrates that three distinct trust infrastructures can - and must operate together in a complementary manner, rather than competing for dominance:

European Blockchain Services Infrastructure (EBSI) provides the engine for new public sector credentials requiring permanent verifiable records and strong governmental oversight. Education credentials-diplomas that must remain verifiable for decades even if issuing universities merge or close-demonstrate EBSI's value. The infrastructure establishes common governance frameworks across countries, eliminates bilateral agreement requirements, and enables privacy-preserving verification where registries provide status information without notifying issuers about every verification event.

Traditional PKI and eIDAS Trust Services anchor legacy credentials with decades of proven reliability. Social Security institutions managing European Health Insurance Cards and Portable Document A1 forms operate mission-critical systems managing legally binding entitlements. These institutions cannot abandon twenty-plus years of PKI infrastructure investment and operational knowledge. The architecture respects these realities, adding EUDI Wallet capabilities without forcing disruptive replacement.

OpenID-based protocols and VC-aware service providers provide the verification layer essential for sectors requiring institutional autonomy. The successful integration with eduGAIN, linking seventy-five academic federations serving millions of researchers, demonstrates how the EUDI Wallet works with established systems through translation bridges. Universities consume high-assurance wallet credentials while maintaining existing SAML-based identity infrastructure, enabling evolutionary transformation rather than forced disruption.

This pluralistic approach is the only viable path to institutional adoption. Attempting to mandate a single trust model would fail not from technical inadequacy but institutional impossibility. The architecture accommodates institutions at different points in their digital transformation journeys through a **bridge pattern** that respects existing investments while enabling high-assurance interoperability

Technical validation is comprehensive: Credentials issued through one trust model are verified successfully through another. Spanish university diplomas verified by Dutch institutions. Polish workers' social security documents verified by French employers. Italian students' enrolment status is recognised by German service providers. Spanish medical doctors’ qualifications accepted in Lithuanian electronic prescription platforms. Seventy percent first-attempt success rate across twelve Member States with zero prior coordination proves the technical foundation is sound. Cryptographic verification completes in seconds (thirteen seconds for complete EHIC verification pluralistic versus thirty minutes traditionally). Privacy protection operates architecturally through selective disclosure - citizens prove specific facts without revealing complete credentials.

Five Barriers Blocking the Path to Production at Scale

Empirical evidence from DC4EU and comparable European digital infrastructure initiatives indicates that successful transition from large-scale piloting to sustainable, pan-European deployment depends on coordinated action across five interlinked pillars. Observed implementation patterns suggest that the absence or delay of the first three pillars during early deployment phases creates high risks of fragmentation that are difficult and costly to reverse,

while the latter two function as enabling conditions for adoption and scale. Success requires coordinated action across five interlinked pillars. Three must occur in Q1 2026 or the mandate fails:

1. Legal Clarity (Q1 2026 - Critical):

Pilot evidence reveals risk-averse verifier behavior, rejecting compliant foreign credentials or demanding additional verification, stemming from uncertainty about legal obligations and liability. Without authoritative guidance, divergent interpretations become embedded in operational systems, making subsequent harmonisation exponentially more expensive.

The European Commission must publish binding interpretative guidance by March 2026, establishing that Qualified Electronic Attestations of Attributes (QEAAs), Public Body Electronic Attestations of Attributes (PuB-EAAs), and properly accredited non-qualified EAAs receive equivalent legal recognition when meeting comparable assurance standards. Crucially, this guidance must be anchored in the immediate operationalisation of the schema and attribute catalogues mandated by Implementing Regulation (EU) 2025/1569. These catalogues must serve as the definitive source for the interoperability, data model, governance, and trust specifications required for both public and private entities to begin technical integration. A standardised verifier liability framework must clarify that accepting compliant foreign credentials following standard verification procedures creates no greater liability than accepting domestic equivalents.

While eIDAS 2.0 mandates cross-border recognition, enforcement depends primarily on Member State supervisory bodies. To bridge the gap between regulation and adoption, the Commission must urgently prioritise filling these currently absent attribute catalogues. This is the only path to building market awareness and providing public and private institutions with the operational tools necessary to start integrating with EUDI Wallets. The Commission's essential coordination role, issuing guidance, initiating infringement proceedings, and fostering supervisory cooperation, must be complemented by robust Member State regulatory action ensuring consistent acceptance obligations are enforced at the operational level where verification decisions occur daily.

2. Harmonised Governance (Q1 2026 - Critical):

Large-scale pilots consistently show that technical interoperability alone does not prevent fragmentation when governance authority is diffuse. In the absence of clearly mandated and operationally focused coordination, Member States and sectors tend to optimize locally. This leads to incompatible metadata profiles, divergent implementation choices, and sector-specific exceptions that undermine the "Common Toolbox" philosophy of the ARF.

Empirical experience from DC4EU and earlier EU digital infrastructure projects indicates that achieving cross-border scale requires **strengthening and expanding** the European Digital Identity Cooperation Group (EDICG). Established under Article 46e of the revised eIDAS Regulation (Regulation (EU) 2024/1183), the EDICG must be empowered with genuine political and operational mandate to align implementation decisions across all Member States.

Rather than serving solely as a consultative forum, **the EDICG should be transformed into** the central coordination authority responsible for:

- **Enforcing Convergence**: Coordinating common metadata standards and populating the attribute catalogues required by IR 2025/1569
- **Directing ARF Evolution**: Managing dynamic evolution of the Architecture and Reference Framework based on real-time pilot evidence

- **Mediating Conflicts**: Resolving cross-sectoral technical conflicts before they become embedded in national law
- **Escalating Critical Barriers**: Ensuring unresolved technical or legal blockages are escalated to political level with sufficient urgency

Evidence from comparable programmes suggests that once divergent national design paths are operationalized, retroactive alignment requires substantially greater effort and cost - typically three to five times more - than early, mandated coordination through a strengthened EDICG.

3. Sustainable Funding (Q1 2026 - Critical):

Pilot experience provides direct empirical evidence that discontinuous or short-term funding undermines institutional capacity, leading to loss of specialised staff, erosion of operational knowledge, and reversion to maintenance-only modes. In DC4EU, gaps between pilot funding and follow-on financing were associated with measurable capacity loss among participating institutions.

Sustained deployment therefore depends on predictable, multi-annual production funding mechanisms that support both core European infrastructure and institutional integration capacity. Evidence from EU infrastructure programmes indicates that funding horizons shorter than multiple years are insufficient for staffing, procurement, and long-term system operation.

Without timely transition from pilot to production funding, accumulated implementation capability deteriorates in ways that cannot be rapidly reconstituted..

4. Architectural Interoperability (Mid-2026 - Enabling):

While pilots demonstrate technical feasibility of cross-border verification, they also reveal that institution-by-institution integration based on bespoke mappings is economically unsustainable at scale. Observed integration costs and effort vary widely, but consistently increase barriers for smaller or less digitally mature institutions.

Empirical evidence from DC4EU and comparable interoperability initiatives supports the value of shared infrastructure components, such as harmonised schema catalogues, governance mapping services, common verification interfaces, and reusable integration tooling. Availability of such components substantially lowers marginal integration effort and reduces variability across implementations.

In the absence of shared interoperability infrastructure, comprehensive coverage across institutional landscapes becomes economically and operationally constrained..

5. Citizen Trust (Mid-2026 - Enabling):

User testing and operational observations indicate that citizen adoption is highly sensitive to workflow complexity, manual fallback processes, and unclear error handling. Systems that require users to act as “data couriers” or that fail silently during verification consistently generate distrust and abandonment.

Empirical findings support the need for automated verification workflows, selective disclosure by default, and transparent user feedback mechanisms. Usability benchmarks derived from pilot experience and comparable digital public services indicate that a substantial majority of representative users must be able to complete common tasks independently for sustained adoption to occur.

Failure to address user experience and trust at deployment stage does not typically block initial rollout, but it reliably undermines long-term usage and legitimacy.

The Stark Choice

Europe has the blueprint. The technology works. The architecture accommodates institutional diversity **through the bridge pattern**, maintaining interoperability while preserving existing federation investments. The legal framework supports automatic cross-border recognition. Three years of intensive piloting across twenty-five countries answered the technical questions.

What remains is execution. The Commission must launch a dedicated Deployment Funding Call immediately. Member States must commit political will and resources to coordinated deployment. The Governance Board must be operational by Q1 2026.. Legal guidance must be published by March 2026. The Harmonisation Layer must be deployed by June 2026. These are not aspirational goals: they are prerequisites for meeting the legal mandate twelve months away.

The alternative is clear: fragmentation into incompatible national implementations failing to deliver cross-border interoperability, institutional atrophy as capabilities built over three years dissipate, citizen distrust as poor user experience drives abandonment, and ultimately failure to meet the 2026 mandate with broader consequences for European digital sovereignty.

DC4EU demonstrated that the EUDI Wallet can work. Whether it will work at scale depends entirely on decisions made in the next three months. The technical foundation is ready. The question is whether Europe is ready to execute.

1 Scope: The Critical Window for Execution

All Member States are legally mandated to issue at least one functional EUDI Wallet by the end of 2026. There is less than 12 months to get this right.

The revision of the eIDAS Regulation (eIDAS 2.0) and the introduction of the European Digital Identity (EUDI) Wallet represent a fundamental paradigm shift toward a citizen-centric digital single market. This transition requires more than technical tools and standardised protocols. It demands decisive political action and unified strategic execution across institutions, Member States, and the European Commission itself.

The purpose of this policy paper is to systematically analyse the DC4EU experience through the lens of what **policymakers, institutional leaders, and sectoral regulators** need to understand about the transition from pilot to production.

The document draws on detailed technical protocols, regulatory requirements, and institutional perspectives gathered during over more than two years of real-world piloting activity across two critical domains:

- **Education:** piloting digital academic credentials, digital diplomas, and professional qualifications in regulated professions.
- **Social Security:** piloting essential cross-European entitlements represented by the European Health Insurance Card (EHIC) and Portable Document A1 (PDA1) forms.

The pilot validated technical feasibility, but more importantly, it exposed what is needed to bridge the gap between a working prototype and a production system serving 450 million citizens.

This document identifies five essential pillars required for production-scale execution. Legal clarity must prevent the rejection of valid credentials lacking technical interoperability about issuers' competencies, verifiers' rights and credential holders. Harmonised governance must establish a top-level authority capable of enforcing common standards. Sustainable funding must replace short-term project grants with the multi-annual operational budgets that infrastructure requires. Architectural interoperability must provide the tools that enable legacy system integration. Citizen trust must be preserved through a user-first design that eliminates unnecessary friction.

These are not aspirational recommendations for future consideration. They represent the documented gap analysis emerging from 101 institutions testing the system under real conditions. Without addressing all five pillars, the 2026 mandate shifts from operational reality to aspirational policy that Member States will struggle to implement coherently.

The findings in this document clarify the governance, legal, and operational changes that must be implemented immediately to guarantee the long-term institutionalization and sustainability of the EUDI Wallet. The strategic imperative is both clear and urgent: transform these insights into coordinated execution or accept that Europe's digital sovereignty ambitions will fragment into twenty-seven incompatible national approaches that fail to deliver on the promise of seamless cross-border digital services.

Terminology and Scope Clarification

Throughout this document, references to "high assurance" credentials describe technical and operational assurance characteristics (such as identity proofing, cryptographic protection, and lifecycle control) and do not imply legal equivalence between different categories of Electronic Attestations of Attributes under Regulation (EU) 2024/1183 (revised eIDAS). In particular, Public Body Electronic Attestations of Attributes, Qualified Electronic Attestations of Attributes, and non-qualified Electronic Attestations of Attributes remain legally distinct instruments with different supervisory regimes and legal effects, even where their technical assurance properties

may be comparable. All statements concerning recognition and acceptance are to be understood as subject to the applicable eIDAS and sectoral legal frameworks.

What This Report Provides

This report serves multiple audiences with diverse needs:

For policymakers and political leadership: Sections 5-6 document five systematic barriers preventing production deployment (unsustainable funding, legal fragmentation, technical interoperability gaps, governance fragmentation, user experience failures) and propose five coordinated action pillars addressing each barrier directly. Three actions must occur in Q1 2026 - establishing governance, securing funding, publishing legal guidance - or the mandate fails.

For technical implementers and institutional leaders: Sections 2-4 explain the architectural foundation enabling pluralistic coexistence of EBSI, PKI/eIDAS, and OpenID Federation, document successful pilot implementations across Education and Social Security domains and provide concrete examples of working user journeys demonstrating technical viability.

For governance and oversight bodies: Sections 7-8 define Key Performance Indicators measuring success across quantitative impact targets (verification success rates, processing time reduction, citizen adoption) and qualitative alignment milestones (legal clarity, governance maturity, institutional readiness), paired with a phased roadmap specifying actions, owners, deadlines, and dependencies.

2 Background: The EUDIW Paradigm

The European Union is advancing toward a vision of digital sovereignty that fundamentally reimagines how citizens prove their identity, share personal data, and access services across borders. This vision centres on enabling citizens to interact with both public and private services seamlessly throughout the Union while maintaining genuine control over their personal information. The transformation is anchored by the European Digital Identity Wallet (EUDIW), representing a fundamental shift away from delegated third-party authentication toward a model focused squarely on user control and self-authentication.

"Instead of asking Google, Facebook, or even your bank to vouch for who you are, the EUDI Wallet lets you prove it yourself: directly, securely, and with complete control over what information you share."

For decades, digital identity has operated through intermediaries. Citizens prove who they are by asking trusted organisations – government agencies, universities, banks - to vouch for them to other parties. This delegation creates dependencies where citizens cannot prove their identity if the intermediary is unavailable, cannot control what information the intermediary shares, and have limited visibility into how their identity assertions are being used. The EUDIW inverts this model by placing cryptographically verifiable credentials directly in citizens' hands, enabling them to prove facts about themselves without requiring real-time permission from the organisations that originally attested to those facts.

The DC4EU large-scale pilot served as the critical testing ground for translating this vision from regulatory text and technical specifications into operational reality across Education and Social Security domains. Although early European identity initiatives often centred on single infrastructure solutions such as the European Blockchain Services Infrastructure (EBSI), the DC4EU consortium learned through direct implementation experience that effective deployment requires embracing rather than minimising Europe's institutional diversity. The project strategically moved beyond attempts to standardise on one model, instead addressing the EU's diverse institutional requirements through what emerged as the necessary architectural approach.

The consortium successfully validated what we now term a *Pluralistic Coexistence Strategy*, demonstrating that effective EUDIW deployment requires three distinct trust frameworks to work together rather than compete for dominance. This pragmatic approach was not predetermined in project planning documents but emerged from encountering real institutional requirements and constraints. The strategy confirmed the viability of three complementary trust infrastructures working as an integrated system.

1. **EBSI:** The project strategically used the European Blockchain Services Infrastructure (EBSI) to issue and verify high-assurance digital credentials within defined public sector domains. This infrastructure successfully piloted the creation of credentials such as Digital Diplomas and Academic Credentials issued as Public Body Electronic Attestations of Attributes (PuB-EAAs), particularly within the Education domain, where the governance structure is more closed. These credentials root themselves in state authority and governmental oversight, drawing their legal force from the public sector bodies that issue them.

   The EBSI-based approach proved particularly well-suited for the Education domain. Following strategic consideration of the binding legal and regulatory requirements for the Social Security pilot, which relies on the eIDAS framework's traditional PKI/eIDAS processes, specifically Qualified Electronic Seals (QES) to issue mandatory, high-assurance PuB-EAAs (e.g., EHIC and PDA1) that must comply with the QEAA standard, the decision was made to exclusively use the PKI infrastructure for that use case. The successful validation of both EBSI and PKI highlights the technical need for the Pluralistic Coexistence Strategy.

2. **Traditional PKI and eIDAS Trust Services:** These provide the foundational trust layer for social security coordination credentials issued as Public Body Electronic Attestations of Attributes (PuB-EAAs). The project confirmed that legacy-anchored competent institutions acting as authentic sources can be seamlessly integrated into the EUDI Wallet ecosystem for this particular legal regime through new architectural layers, rather than being required to replace their existing technical systems. Credentials such as the European Health Insurance Card (EHIC) and the Portable Document A1 (PDA1) represent substantial institutional investment and long-standing operational practice. This history does not justify replacement where current systems—often based on established formats such as paper or plastic cards—continue to function reliably. The overall architecture therefore accommodates these traditional credentials inclusively, while enabling a gradual evolution toward registry-based verification models when institutions are technically and operationally ready..
3. **OpenID Federation:** The project employed the OpenID framework as the vital verification and federation layer for sectors requiring greater institutional autonomy, such as education and research. This framework successfully integrated the EUDIW with established academic identity networks like eduGAIN, demonstrating a crucial bridge for cross-border verification that respects existing institutional governance structures. The integration allows universities to maintain their federated identity systems while consuming high-assurance EUDI Wallet credentials, providing evolutionary transformation rather than disruptive replacement.

"Think of it like Europe's electrical system. EBSI is like new high-voltage infrastructure for major installations. PKI is the existing grid that has been reliable for decades. OpenID Federation is the smart adapter that lets everything work together. You need all three: trying to replace the existing grid overnight would leave half of Europe in the dark."

The successful demonstration of interoperability among these three frameworks confirmed that the Architecture Reference Framework (ARF) must be capable of facilitating this coexistence, rather than mandating uniformity. The ARF must ensure flexibility while demanding the harmonisation necessary to address governance equivalency and assurance comparability across different technical approaches. The technical foundation draws upon protocols including OpenID Connect (OIDC), OIDC4VCI for credential issuance, and OIDC4VP for credential presentation, ensuring alignment with modern, scalable, and privacy-preserving standards that have been proven at internet scale.

2.1 The Legal Foundation: eIDAS 2.0 and GDPR

The legal foundation for Europe's shift toward citizen-controlled digital identity rests on two complementary regulatory frameworks that together establish both the trust infrastructure enabling cross-border recognition and the privacy protections ensuring citizens retain meaningful control over their personal data.

The revised eIDAS Regulation, formally adopted in May 2024 as Regulation EU 2024/1183, provides the trust framework upon which the entire EUDI Wallet ecosystem is built. This regulation expands substantially upon its predecessor, the original eIDAS Regulation from 2014, which established a legal framework for electronic identification and trust services but did not envision the wallet-based model now being deployed (even if the so-called middleware approach, based in smartcards shares many of the functional objectives of the EUDI Wallet). The revised regulation introduces a comprehensive legal framework for the issuance, recognition, and use of EUDI Wallets across Member States, explicitly mandating the wallet as a legally recognised instrument that Member States must provide to their citizens and residents.

The regulation defines detailed requirements for Electronic Attestations of Attributes (EAAs) in their various forms. Qualified Electronic Attestations of Attributes issued by Qualified Trust Service Providers receive the strongest legal protections and automatic mutual recognition.

Public Body Electronic Attestations of Attributes (PuB-EAAs) issued directly by authentic sources within public sector organisations carry specific legal characteristics due to a transparent and explicit mandate by law, which anchors their legal force in their governmental origin.

Non-qualified Electronic Attestations of Attributes issued by other trusted entities serve important functions where the full qualified or public body frameworks are not necessary or proportionate. Understanding these distinctions matters for policy implementation even though the credentials often look similar from citizens' perspectives.

Most fundamentally, the revised eIDAS establishes the framework for cross-border mutual recognition, transforming digital credentials from national documents requiring foreign approval into European instruments designed for use across borders and business domains. When a credential complies with the applicable eIDAS provisions and relevant sectoral law, it provides the legal and technical assurance necessary for cross-border recognition within that framework. This approach aims to remove the discretion that would otherwise allow national authorities to reject foreign credentials simply because they are unfamiliar or issued through different technical mechanisms.

The General Data Protection Regulation provides the essential privacy framework ensuring that legal certainty about identity does not come at the cost of surveillance and loss of privacy. GDPR establishes comprehensive requirements for how personal data is processed, with specific principles directly shaping the EUDI Wallet's architecture. The integration of eIDAS 2.0 and GDPR ensures that all data shared through the wallet is subject to explicit user consent, meaning citizens must actively approve each sharing action rather than providing blanket permission. Data minimization requires that only information strictly necessary for each specific purpose can be requested and shared. Purpose limitation prevents credentials shared for one purpose from being repurposed for unrelated uses without separate consent.

The GDPR principles manifest in concrete architectural decisions throughout the EUDI Wallet design. Privacy by Design is not a compliance checklist completed after system development but a fundamental approach where privacy protections are embedded in the system's basic operation. Privacy by Default means that the most privacy-protective settings apply automatically rather than requiring citizens to discover and activate privacy features. These principles ensure that doing the privacy-protective thing is easier than doing the invasive thing, reversing the usual pattern where privacy requires constant vigilance and effort while surveillance happens automatically.

Throughout Sections 1 through 5, we use "QEAA" as shorthand when discussing high-assurance credentials generally, since from technical and operational perspectives these credential types share more similarities than differences. However, this convention is suspended in Sections 6 and 7, where policy recommendations demand legal precision. There, the distinctions between Qualified Electronic Attestations of Attributes from Qualified Trust Service Providers, Public Body Electronic Attestations of Attributes from government authentic sources, and properly accredited non-qualified Electronic Attestations of Attributes become critical.

This distinction matters because current practice reveals troubling patterns of credential discrimination. The eIDAS legal framework explicitly mandates non-discrimination and supports equivalence across different issuance models when they meet comparable standards (e.g., accepting a high-assurance Public Body EAA alongside a QEAA, provided both meet the required assurance level).

However, verifiers sometimes violate this core principle by refusing credentials that meet all legal requirements simply because they were issued through unfamiliar technical mechanisms. For

instance, a high-assurance credential from a university acting as an authentic source might be rejected in favour of demanding a Qualified Electronic Attestation of Attributes (QEAA) from a Qualified Trust Service Provider, even when both provide equivalent assurance.

This operational discrimination contradicts the fundamental policy goal of enabling seamless cross-border credential use based on actual assurance levels rather than technical implementation details. Section 6 addresses this gap between the legal mandate and operational practice, arguing that the core principle of non-discrimination and legal equivalence must be robustly enforced, rather than merely stated in regulations that verifiers currently interpret restrictively.

2.1.1 Governance Roles: Commission vs. Member States in EAA/QEAA

Understanding the policy recommendations and technical findings requires clarity about the governance obligations assigned to the European Commission versus those assigned to Member States under the amended eIDAS Regulation. This separation of responsibilities is not merely administrative detail but reflects fundamental questions about where authority resides for different aspects of the trust infrastructure. The distribution of responsibilities becomes particularly important for the high-assurance credentials that DC4EU piloted: the Qualified Electronic Attestations of Attributes (QEAA) and Public Body Electronic Attestations of Attributes (Pub-EAA) governed by Articles 45 and 45f of eIDAS 2.0.

Table 1: European Commission vs Member State Governance Roles

Responsibility	European Commission (EC) Role	Member States (MS) Role
Qualified Trust Services (QTSPs/QEAA)	Maintains and publishes the Union Trusted Lists for qualified trust services and QTSPs. This creates a single authoritative source where any party can verify whether a particular trust service provider holds qualified status and what services they are authorised to provide.	Supervise Trust Service Providers and notify QTSPs and their qualified services for inclusion in national Trusted Lists. National-level supervision of Trust Service Providers operating under their jurisdiction, conducting the audits and assessments that determine whether providers meet the strict requirements for qualified status. When providers satisfy requirements, notify them to EC for inclusion in national Trusted Lists that feed into the Union list.
Public Body EAAs (PuB-EAA)	Publishes, in sealed machine-readable form, the list of public sector bodies acting as Authentic Sources and authorised to issue EAAs (as notified by MS). This publication occurs based on notifications from MS rather than the EC making independent determinations about which bodies qualify.	Identify which public sector bodies should be recognised as Authentic Sources. Ensure those bodies meet reliability and trustworthiness requirements equivalent to what Qualified Trust Service Providers (QTSPs) must meet for their respective scopes and notify them to the Commission for publication[1].

[1] The equivalence requirement establishes that public bodies issuing Electronic Attestations of Attributes must meet standards comparable to Qualified Trust Service Providers even though they are not subjected to identical procedures. A ministry issuing professional qualifications or a social security agency issuing entitlement documents must implement security, privacy protection, and operational reliability measures that are appropriate to the sensitivity and legal significance of what they issue. The regulatory approach recognises that subjecting government ministries to the same third-party audit requirements applicable to commercial trust service providers would be inappropriate given their different legal status, but it does not excuse them from meeting equivalent substantive standards.

Standards & Implementation	Adopts implementing acts defining technical standards and operational procedures applicable to QEAA and EAAs issued by or on behalf of public sector bodies. These implementing acts provide the detailed specifications that the regulation itself cannot contain, translating high-level legal requirements into concrete technical and procedural standards.	Ensure that these public bodies provide interfaces towards EUDI Wallets for issuing EAAs. The technical integration cannot be left to chance or voluntary adoption but must be systematically implemented.
Attribute Validation	N/A	With the data subject's consent, Qualified Trust Service Providers issuing Qualified Electronic Attestations of Attributes must be able to validate attributes against Authentic Sources maintained by public sector bodies. A qualified trust service provider issuing a credential attesting to someone's professional qualification needs to verify that information against the registry maintained by the licensing authority. Member States must establish the technical and legal frameworks making such validation possible while respecting data protection requirements and ensuring that validation occurs only with appropriate consent.

"The Commission sets the rules and maintains the master lists. Member States operate the systems and vouch for their trustworthiness. Both roles are essential – and both create accountability points."

This distribution of responsibilities creates a complex governance environment where neither the Commission nor individual Member States can act unilaterally to ensure system success. The Commission can establish standards and maintain central registries, but it depends on Member States to implement those standards and populate the registries with accurate information. Member States can designate Authentic Sources and supervise trust service providers, but their efforts have limited value if other Member States do not recognise the resulting credentials or if the Commission fails to maintain effective coordination mechanisms. Success requires sustained cooperation across levels of governance rather than top-down mandates or purely voluntary coordination.

2.2 Core Features of the EUDIW and User Sovereignty

Credentials issued to a European Digital Identity Wallet (EUDIW) constitute legally recognised Electronic Attestations of Attributes within the meaning of Regulation (EU) 2024/1183 and its implementing acts, provided they are issued, managed, and verified in accordance with the applicable trust, governance, and lifecycle requirements. Their legal effect derives from compliance with the eIDAS framework and relevant sectoral law, rather than from solution-specific or proprietary mechanisms.

The EUDI Wallet's architecture enables four critical, interlinked features that transform digital interactions: mutual authentication to establish trust, robust lifecycle management (revocation and suspension) to mitigate fraud, machine-enforced policy implementation to restrict data access, and flexible verification and usage concepts.

1. Mutual Authentication and Trust

Security and privacy safeguards are ensured by design through the standardised EUDI Wallet architecture. The wallet enables mutual authentication between issuer, holder, and verifier, establishing a trusted three-party interaction in which the issuer is cryptographically authenticated, the verifier is authenticated to the wallet before any data disclosure occurs, and the holder retains control over credential presentation. This mutual trust model ensures that credentials are disclosed only to authorised and identifiable verifiers and only from authenticated issuers.

2. Lifecycle Management (Revocation and Suspension)

The EUDI Wallet is identity-bound and state-aware, supporting full credential lifecycle management, including issuance, validity enforcement, suspension, and revocation. Credential status can be updated or invalidated to mitigate fraud, error, or changes in entitlement, and verifiers can reliably determine current validity using trusted status information, without requiring continuous issuer involvement.

3. Policy-Based Access Control

Policy-based access control is implemented at multiple levels. Issuers define conditions under which credentials may be used; verifiers specify legally and contextually justified data requests; and the wallet enforces these policies through explicit user consent, selective disclosure, and purpose limitation. Access to data is therefore restricted by machine-enforceable policies aligned with eIDAS and GDPR requirements, ensuring that only the minimum necessary information is disclosed for a given use case.

4. Flexible Verification and Usage Concepts

Because the EUDI Wallet supports interactive, policy-driven verification, it enables a wide range of flexible validity and usage concepts, including one-time presentation, short-lived credentials, usage-limited attestations, context-bound access, and dynamic suspension or reactivation. These capabilities allow credentials to be adapted to diverse legal and operational requirements across sectors, while preserving security, interoperability, and user sovereignty.

Together, these features transform the EUDI Wallet from a passive container for credentials into an **active trust instrument** that enables secure, privacy-preserving digital interactions. Citizens act as custodians of their credentials, while issuers and verifiers operate within a common, legally governed trust framework that ensures authenticity, prevents fraud, and supports cross-border use.

"The EUDI Wallet shifts power from service providers to citizens. You become the custodian of your own digital identity - not just another user in someone else's database."

2.3 The Strategic Context: Architecture Reference Framework (ARF)

The Architecture and Reference Framework (ARF) constitutes the foundational technical pillar and a central political instrument of the European Digital Identity system. As the Union's "Common Toolbox," it defines harmonised specifications that Member States and ecosystem actors are expected to implement to enable secure, trusted, and interoperable EUDI Wallet deployments. The ARF therefore reflects political decisions about standardisation and interoperability, rather than serving merely as descriptive technical guidance.

The ARF's core objective is to mandate structured cooperation between ecosystem actors—issuers, verifiers, wallet providers, and wallet holders—by defining common credential formats, interaction

protocols, and assurance expectations. Issuers, including public authorities, educational institutions, and private organisations acting as qualified or non-qualified issuers under eIDAS, are expected to format credentials and expose interfaces in line with ARF specifications. Verifiers are expected to implement ARF-specified verification protocols, while wallet providers must implement security, privacy, and user-experience requirements that allow credentials issued in one Member State to be presented and verified in another.

The ARF coordinates multiple dimensions of the ecosystem. Wallet interface specifications aim to prevent fragmentation in user interaction patterns across Member State implementations. Protocol specifications, based on OpenID Connect and its extensions for verifiable credential issuance and presentation, define how credentials and presentation requests flow between issuers, wallets, and verifiers. Credential format specifications drawing on the W3C Verifiable Credentials Data Model enable verifiers to interpret credentials independently of national or institutional origin. Common assurance profiles seek to establish comparability across different technical trust models by defining assurance in operational terms, including identity binding, authentication strength, and lifecycle controls.

Empirical evidence from DC4EU confirms that the ARF is a necessary but not sufficient condition for successful deployment. Pilots demonstrated that technical compliance with ARF specifications does not automatically translate into institutional readiness, adoption, or operational sustainability. In particular, DC4EU identified verifier onboarding as a critical success factor: many verifiers are private-sector organisations, including educational institutions, healthcare providers, employers, and service operators, whose willingness to rely on wallet-based credentials depends on legal certainty, integration effort, and operational clarity rather than on protocol compliance alone.

This finding aligns with experience from other European large-scale pilots, which have already executed private-sector use cases in domains such as travel, payments, and banking. These initiatives demonstrate that private-sector verification is not an edge case but a core requirement for achieving scale. Revised eIDAS explicitly accommodates this reality by regulating the issuance of Electronic Attestations of Attributes beyond public bodies, including both qualified and non-qualified EAAs issued by private-sector actors under defined trust and governance conditions.

DC4EU further showed that when multiple trust models coexist—public-sector issuance, qualified trust services, and non-qualified private issuance—formal interoperability at protocol level is insufficient on its own. Without shared semantic interpretation, governance alignment, and practical onboarding support, verifiers tend to implement parallel logic, bespoke mappings, or restrictive acceptance policies, increasing cost and fragmentation. This indicates that the ARF must be complemented by operational governance, harmonisation tooling, and verifier-focused guidance to ensure that its specifications translate into effective cross-sector adoption.

The ARF deliberately builds on established global standards, including the W3C Verifiable Credentials Data Model, OpenID-based protocols, ISO/IEC identity management standards, and ETSI trust service specifications. Empirical experience confirms that leveraging these standards reduces technical risk and facilitates international interoperability. At the same time, DC4EU evidence highlights that the principal challenge is not the selection of standards, but their consistent operationalisation across heterogeneous institutional and commercial environments. The Strategic Role of DC4EU

The Digital Credentials for Europe (DC4EU) project served as the primary vehicle for stress-testing the EUDI Wallet's legal and technical innovations under real-world conditions for PUB-EAAs. The project brought together 101 institutions from twenty-five countries to answer one fundamental question:

Can the EUDI Wallet actually work for Europe's most critical public services when deployed at scale across diverse institutional contexts, legal frameworks, and technical infrastructures?

DC4EU's scale distinguished it from typical pilot projects. The project deliberately included institutions of varying sizes and sophistication - from major research universities to small municipal governments, from national social security agencies to regional training centres. This diversity ensured findings would reflect real implementation challenges rather than optimistic results from only the most capable participants.

"If the EUDI Wallet can handle a Polish construction worker getting emergency care in Portugal while working temporarily in France - with three different national systems, two different credential types, and real-time verification requirements - then we know the architecture is production-ready."

The project concentrated on two strategic domains representing dramatically different institutional environments. Education and Professional Qualifications encompassed comprehensive lifelong learning: digital diplomas from universities, professional qualifications for regulated professions, vocational training credentials, and micro-credentials for labour market upskilling. The Social Security domain focused on two high-impact documents - the European Health Insurance Card enabling cross-border medical treatment and the Portable Document A1 certifying social security coverage for temporary cross-border work. Both carry legal and financial significance far beyond administrative convenience.

These domains were chosen strategically to test the EUDIW across a spectrum of operational and governance realities.

- **Education institutions and professional bodies** typically operate modern IT systems with five-to-ten-year refresh cycles and a high innovation appetite. They follow a **federated governance** model that respects institutional autonomy. Educational credentials often have **decades-long lifecycles.**
- **Social Security** operates a complex and **highly heterogeneous infrastructure**, combining legacy systems with modern, decentralised systems (e.g., using state-of-the-art concepts such as eID, federated governance in some cross-border contexts, and service-oriented architecture). These systems represent massive national investments, handle legally binding entitlements, and therefore approach change cautiously. They primarily follow a **centralised national governance** model with ministerial directives. Social Security entitlements change **dynamically, potentially monthly.**

The contrast between the two domains, where one prioritises innovation and autonomy (Education), and the other prioritises caution and legal certainty (Social Security), allowed DC4EU to validate the EUDIW's ability to function reliably across fundamentally different public-sector environments.

If the EUDI Wallet could function across both these dramatically different environments, the architecture could reasonably handle the full spectrum of European institutional diversity. Conversely, failure in either domain would signal fundamental gaps requiring resolution before widespread deployment.

The EUDI Wallet's interactive nature and standardised protocols also introduce a powerful incentive: the ability to create innovative new services and streamlined processes that are triggered by a secure wallet interaction. This potential for new business cases and operational efficiencies can serve as a strong incentive for both public and private stakeholders to onboard, generating value that goes beyond mere compliance or credential storage.

DC4EU's validation achievement extends across multiple dimensions. Technical feasibility was demonstrated through successful cross-border issuance and verification with different trust models. Legal validity was established through GDPR, eIDAS, and national regulation compliance. Institutional viability was proven by integrating with existing systems like eduGAIN federations and national PKI infrastructures, demonstrating that deployment need not require wholesale replacement. User acceptability was validated through testing showing representative citizens could successfully use wallets without technical expertise.

The strategic contribution extends beyond technical feasibility to generating essential policy feedback refining eIDAS guidelines and ARF specifications. The project identified regulatory gaps, recommended clarifications incorporated into implementing acts, documented integration patterns the ARF now references, exposed governance challenges requiring new coordination mechanisms, and validated privacy-preserving techniques.

The recommendations in Sections 5 to 8 draw directly from the DC4EU experience and the many organisations and industry leaders involved in different work packages. The five systemic barriers in Section 5 emerged from observing where institutional progress stalled despite technical capability. The five action pillars in Section 6 respond to specific gaps preventing pilot successes from scaling to production. The performance indicators in Section 7 reflect what actually proved measurable rather than theoretical metrics. The phased roadmap in Section 8 sequences actions based on observed dependencies rather than idealised templates.

DC4EU transformed the EUDI Wallet from regulatory mandate into a proven, deployable system tested under real-world conditions with real institutions, credentials, and citizens. The evidence base grounding this report represents three years of intensive implementation experience across twenty-five countries involving more than one hundred institutions. The findings have credibility because they emerge from operational reality rather than speculation.

“DC4EU was not just a pilot: it was Europe's dress rehearsal for 2026. We found what works, what breaks under pressure, and what needs fixing before 27 Member States deploy to 450 million citizens.”

3 Operational Success: The Pluralistic Coexistence Blueprint

The DC4EU project achieved critical operational success by moving decisively beyond technical proof-of-concept demonstrations to deliver an institutionally viable architectural blueprint for the EUDIW. The accomplishment extends beyond validating that protocols function correctly or that credentials can be cryptographically verified. The project proved that the system could work across the institutional diversity, legal complexity, and technical heterogeneity that characterise the European Union in practice rather than in idealised models assuming uniform capabilities and approaches.

The fundamental discovery emerging from this work was not anticipated in project planning documents but emerged as the necessary conclusion from encountering real-world institutional constraints and requirements.

A single, monolithic trust model cannot meet the diverse legal, governance, and infrastructural requirements across the Digital Single Market. Attempts to mandate universal adoption of one technical approach, whether traditional PKI, blockchain-based registries, or federated identity management systems, would fail to gain institutional acceptance in sectors with substantial existing investments in alternative approaches.

Diversity is not a problem to be solved through standardisation but a reality to be respected through intelligent architecture and pragmatic strategy. Crucially, a monolithic approach would also severely slow down innovation and progress and jeopardise Europe's objective of digital sovereignty by hindering the market's ability to adapt and build diverse technical solutions that meet national and sectoral needs.

The pilots validated this architecture in foundational public domains where failure would have profound consequences for citizens and institutions alike. The project successfully issued and verified high-assurance Electronic Attestations of Attributes across multiple categories. Public Body Electronic Attestations of Attributes issued directly by government agencies and educational institutions demonstrated that public sector bodies could function as authentic sources issuing credentials with governmental authority. Non-qualified Trust Service Provider-based Electronic Attestations of Attributes showed that institutions not qualifying as public bodies or willing to operate as Qualified Trust Service Providers could still issue high-assurance credentials appropriate for their contexts. The Education sector pilots encompassed a comprehensive approach to lifelong learning including Professional Qualifications such as specialised medical training, Vocational Education and Training credentials, Technical and Vocational Education and Training programs, and traditional Higher Education degrees and diplomas.

The Social Security domain confirmed the model's scalability across institutional settings dramatically different from education. Testing the European Health Insurance Card and Portable Document A1 credentials validated that systems managing legally binding entitlements with direct financial and medical consequences could integrate with EUDI Wallets while maintaining the reliability and security that such high-stakes applications demand. The successful demonstrations across both domains confirmed that the architecture could accommodate Europe's institutional variety rather than requiring uniform technical approaches that some sectors would find impossible to adopt.

The resulting architectural decision represented a conscious strategic policy choice to manage complexity through what we term the **Pluralistic Coexistence Strategy**. This was not merely a technical finding about interoperability protocols but a fundamental conclusion about governance models and institutional reality. Europe's existing identity landscape includes too much diversity, too many proven systems, and too many legitimate institutional interests to be forced into a single technical model regardless of how theoretically superior that model might appear.

The project successfully engineered a hybrid architecture integrating three legally and operationally distinct trust management infrastructures. The European Blockchain Services Infrastructure (EBSI) provides registry and governance capabilities particularly suited to new credentials requiring permanent records and strong governmental oversight, acting as an EU-wide trust anchor store, independent from browser providers.. OpenID Federation protocols enable real-time verification and dynamic trust establishment across federated systems respecting institutional autonomy. Traditional Public Key Infrastructure and eIDAS trust services anchor credentials in legally recognised cryptographic frameworks with decades of operational experience and institutional investment. The integration of these three approaches is not redundant complexity but essential architecture reflecting Europe's institutional reality.

This proactive approach goes substantially beyond the basic technical compliance that the Architecture Reference Framework requires. The ARF specifies protocols and data formats ensuring interoperability, but it does not mandate how different trust models should be integrated or how governance should be coordinated across approaches with fundamentally different assumptions. DC4EU filled this gap by demonstrating functioning integration patterns, documenting governance coordination mechanisms, validating that selective disclosure and privacy protection work across all three trust models, and proving that verifiers can handle credentials from any conformant source without requiring advance knowledge of which specific technical approach was used for issuance.

The blueprint provided by DC4EU constitutes the essential foundation for full-scale, production-level deployment across all Member States. The evidence compiled over three years demonstrates that this complex, nuanced approach represents the non-negotiable path to institutional adoption. Attempting to simplify by mandating a single approach would result not in accelerated deployment but in resistance, fragmentation, and ultimately failure to achieve the cross-border interoperability that the entire initiative aims to enable.

An important clarification about pilot scope ensures accurate understanding of what DC4EU validated and what remains for future work. The project provides the definitive technical blueprint for Qualified Electronic Attestations of Attributes and demonstrates full compatibility with future Qualified Trust Service Provider operations. The architecture, protocols, and governance models work equally well whether credentials are issued by qualified trust service providers, public bodies acting as authentic sources, or non-qualified issuers operating under appropriate governance frameworks. For legal accuracy it must be noted that DC4EU itself did not operate a Qualified Trust Service Provider during the pilot phase. The institutions issuing credentials were either public bodies issuing Public Body Electronic Attestations of Attributes or non-qualified issuers operating under the hybrid trust model that the project defined and validated. The demonstrable results rely on the technical viability of these credential types as verified under the project's pluralistic trust architecture.

This scope clarification does not diminish the project's achievements but ensures precision about what was directly tested versus what was validated through architectural compatibility and protocol design. The system is ready for Qualified Trust Service Providers to begin operations using the validated protocols and trust frameworks. The integration work, governance models, and technical specifications apply equally regardless of whether a credential originates from a qualified provider, a public body, or an accredited non-qualified issuer. Future deployment will include all three issuer types operating within the proven architectural framework that DC4EU established.

"We started hoping to standardise on one approach. We ended proving that Europe's strength is embracing multiple approaches - and making them work together seamlessly."

3.1 European Blockchain Services Infrastructure (EBSI)

The European Blockchain Services Infrastructure emerged through DC4EU piloting as the optimal foundational trust layer for new, high-assurance digital credentials requiring strong governmental oversight and permanent verifiable records. EBSI is not simply a blockchain registry: it represents a comprehensive European digital trust framework operating as a Trusted Ledger service under eIDAS 2.0 regulatory authority. The infrastructure includes a family of Verifiable Data Registries providing decentralised, tamper-resistant storage of governance information, credential status data, and trust anchors enabling verification without systematic reference back to issuers.

DC4EU successfully deployed EBSI for secure issuance and governance of Public Body Electronic Attestations of Attributes, demonstrating particular strength in the Education sector. Academic credentials exemplify the use case where EBSI's characteristics provide distinctive advantages. A university diploma remains relevant throughout a person's career, potentially requiring verification forty or fifty years after issuance. The issuing university might undergo mergers, name changes, or even closure during that period, yet the credential must remain verifiable with certainty about its authenticity and issuing authority. EBSI's permanent registry model ensures that governance information, trust anchors, and verification data persist independently of the issuing institution's continued operation in its original form.

EBSI can be deployed to add value to both Governance and Privacy.

EBSI's value extends beyond registry services to establishing a common governance layer across countries and sectoral schemes. The infrastructure defines explicit roles: Root Trusted Accreditation Organisations providing ultimate authority, Trusted Accreditation Organisations operating within specific sectors or national contexts, Trusted Issuers authorised under the governance framework, and various technical roles supporting infrastructure operation. These role definitions create auditable accountability chains essential for high-assurance credentials where questions about authority carry legal consequences.

The governance layer establishes comprehensive policies for the complete credential lifecycle from initial authorisation through final revocation. Onboarding procedures define how new issuers gain authority to participate. Accreditation processes establish quality standards with periodic reviews ensuring continued compliance. Audit mechanisms enable oversight verification. Issuance policies define what credentials can be issued, to whom, and under what conditions. Suspension and revocation procedures provide mechanisms for temporary or permanent invalidation when necessary.

These governance capabilities function across national boundaries through EBSI's ‘European scope’ rather than requiring bilateral agreements between institutions. A Spanish university can issue credentials that a German employer verifies without requiring specific agreements between those parties. The governance framework establishes multilateral trust through common standards and oversight rather than through pairwise relationships that scale poorly as participants grow.

EBSI supports enhanced Privacy by Design through architectural choices fundamentally different from traditional PKI approaches. Traditional credential verification often requires verifiers to contact issuing authorities directly, querying revocation services or downloading certificate revocation lists. These direct contacts create privacy vulnerabilities because issuers learn when and where credentials are being verified, enabling surveillance of credential usage patterns and building detailed profiles of how credential holders use their credentials.

EBSI's registry-based verification model breaks this surveillance capability by anchoring status and registry entries on distributed ledgers that verifiers can query without systematically contacting issuers. When a German employer verifies a Spanish university diploma, the verification queries the EBSI registry to confirm validity and current status without notifying the Spanish university. This

prevents universities from accumulating data about where graduates seek employment or how frequently they prove their qualifications. The registry provides information necessary for verification while severing the direct communication enabling issuer surveillance.

This approach limits linkability between separate verification events for the same citizen, providing stronger privacy protection than traditional models where issuers potentially receive notifications every time credentials are verified. The EBSI model makes such linkability substantially more difficult by ensuring verification events do not systematically generate records at issuers connecting those events to specific credential holders. The privacy protection operates architecturally rather than depending on policy commitments or legal restrictions that might change.

The registry model also supports independent presentation where credential holders can prove credentials without depending on issuer availability or cooperation. Traditional models requiring issuer contact create dependencies problematic when issuers experience outages, network connectivity is unreliable, or issuers are uncooperative. EBSI's registry model eliminates this dependency-credentials can be verified against the permanent registry even if the original issuer no longer exists or is temporarily unavailable.

The Critical Limitation Discovered.

DC4EU pilots immediately exposed critical limitations in EBSI's universal applicability. The Social Security domain demonstrated strong and legitimate operational preferences for established national PKI-based systems and eIDAS trust lists rather than blockchain registries. Social Security institutions managing EHIC and PDA1 credentials chose not to integrate their core issuance and revocation processes with EBSI infrastructure despite being enabled to do so. This reflected several intersecting factors. These institutions have operated PKI-based systems for more than twenty years, representing hundreds of millions of euros in investment and accumulated operational knowledge that cannot be replicated quickly. The PKI infrastructure works reliably, handling millions of transactions with legal and financial consequences where failures would be immediately catastrophic. Staff understand PKI workflows, troubleshooting, and security models through years of operational experience.

Legal frameworks in many Member States explicitly reference PKI trust chains and qualified electronic signatures in ways requiring legislative amendments to accommodate alternative trust models. Changing these legal references involves parliamentary processes extending over years. Operational procedures have been optimised around PKI workflows, with interconnections to numerous other systems requiring modification if the underlying trust model changes. The risk management culture in social security institutions favours proven approaches over newer alternatives regardless of theoretical advantages.

The pilot confirmed a critical lesson: **legal compliance with eIDAS 2.0 does not equate to institutional readiness or willingness to abandon proven systems**. Social security institutions using PKI approaches for EHIC and PDA1 credentials were fully compliant with eIDAS requirements. Their credentials met all legal standards for authenticity, integrity, and cross-border recognition. Yet they were not institutionally ready to migrate to EBSI-based issuance despite its technical availability and regulatory blessing.

This critical lesson has policy implications.

A unified trust mandate insisting all high-assurance credentials must be issued through EBSI would have failed not because of technical inadequacy but institutional impossibility. Social security agencies faced with such mandates would have delayed deployment indefinitely, deployed non-compliant systems continuing familiar PKI approaches, or engaged in malicious compliance technically meeting requirements while minimizing actual adoption.

The pluralistic architecture DC4EU validated respects these institutional realities while enabling future flexibility. Social security institutions can continue operating proven PKI systems as foundations for credential issuance, maintaining institutional knowledge and avoiding disruptive replacement. Those same institutions can explore how EBSI-style registries might enhance verification capabilities, provide better privacy protection, or enable new use cases without requiring immediate core system replacement. The architecture allows institutions to adopt EBSI capabilities when ready rather than being forced into premature migration.

Simultaneously, educational institutions finding EBSI's capabilities well-suited to their requirements can leverage those capabilities fully without being constrained by other sectors' preferences. Universities can issue credentials through EBSI gaining all its advantages-permanent verifiable records, strong governance frameworks, privacy-preserving verification - without waiting for social security agencies to complete their adoption journeys.

This discovery and the architectural response represent DC4EU's most significant contribution to European digital identity strategy. The project proved that technical superiority does not determine institutional adoption, that regulatory compliance does not guarantee operational readiness, and that successful deployment requires respecting institutional diversity rather than attempting to eliminate it through standardization mandates. The pluralistic architecture is not a compromise necessitated by political constraints-it is the optimal technical approach for the institutional reality Europe actually faces.

3.2 OpenID Protocols for Interoperability

The suite of OpenID Connect protocols emerged through DC4EU validation as the essential agile layer enabling real-time interaction and verification across the EUDI Wallet ecosystem. These protocols (particularly OIDC4VCI for credential issuance and OIDC4VP for credential presentation) provide standardised communication mechanisms allowing wallets, issuers, and verifiers to interact securely regardless of underlying trust models or technical implementations. The protocols operate at internet scale, proven through billions of authentication transactions before being adapted for verifiable credential use cases.

Understanding Trust versus Exchange Layers

The architecture requires distinguishing clearly between the trust layer and the exchange layer. The trust layer, provided by the pluralistic combination of PKI, EBSI, and eIDAS frameworks, establishes fundamental questions about credential authenticity and validity: Who issued this credential? Is the issuer authorised? Has the credential been revoked? Does the cryptographic signature prove the credential has not been altered? These questions concern trust establishment and status verification.

The exchange layer, provided by OpenID protocols, handles different questions about communication mechanics: How does a wallet request credentials from an issuer? How does a verifier request specific attributes from a wallet holder? How does the wallet present credentials in standardised formats? How are consent and authorisation managed? These questions concern the practical logistics of moving credentials between parties.

Consider a postal mail analogy: PKI and EBSI establish that a sender's signature is authentic and the document has official status - verifying the seal on a government document. OpenID protocols provide the envelope format, addressing conventions, delivery mechanisms, and tracking systems ensuring documents reach intended destinations. Both layers are essential but solve fundamentally different problems at different architectural levels.

The OpenID Protocol Family

OIDC4VCI, the OpenID for Verifiable Credential Issuance specification, enables secure, dynamic interactions between EUDI Wallets and trusted credential issuers. This protocol handles credential creation and distribution, supporting real-time validation and attribute binding during issuance. The protocol supports various issuance flows: immediate issuance when issuers can verify eligibility and generate credentials in real-time, deferred issuance when generation requires human review or external system integration, and batch issuance for efficient processing when institutions issue credentials to many recipients simultaneously. This flexibility allows institutions to use issuance patterns matching their operational capabilities.

OIDC4VP, the OpenID for Verifiable Presentation specification, operates on the verification side. Relying parties use this protocol to request and verify presentations from wallet holders. The protocol supports dynamic requests where verifiers specify exactly what attributes they need, enabling selective disclosure where citizens prove specific facts without revealing unnecessary information. Various interaction patterns accommodate different scenarios: same-device flows where wallet and verifying service operate on the same device, cross-device flows for physical service counters with verification terminals, and offline presentation enabling verification without network connectivity.

The eduGAIN Integration Challenge

The practical importance of OpenID protocols became particularly evident through education sector integration challenges. The eduGAIN federation represents seventy-five national academic identity federations linked through coordinated trust frameworks, handling millions of authentication transactions monthly and becoming essential to European research collaboration. The federation uses SAML, a mature but relatively static standard serving academic identity management for more than fifteen years.

Integrating the EUDI Wallet with eduGAIN required bridging between the wallet's credential model using verifiable presentations and eduGAIN's SAML-based infrastructure using authentication assertions. Forcing all eduGAIN participants to abandon SAML for entirely new protocols would have created massive disruption. Universities had invested substantially in SAML-based systems, trained staff on those systems, and built processes depending on SAML's characteristics. Demanding wholesale replacement would have generated resistance that no amount of technical argumentation could overcome.

DC4EU engineered a bridge solution introducing a VC-aware Service Provider that translates between models. This bridge accepts verified credential presentations from EUDI Wallet holders using OIDC4VP, validates credentials against appropriate trust registries, extracts relevant attributes, and converts them into SAML assertions that relying institutions consume through existing identity management systems without modification.

From the university infrastructure perspective, nothing changes: the system receives SAML assertions formatted identically to those processed for years. From the citizen's perspective, they present credentials from a modern, privacy-preserving EUDI Wallet with selective disclosure and user control. The bridge handles translation invisibly, maintaining backward compatibility while enabling forward progress. This exemplifies evolutionary transformation respecting existing investments while introducing new capabilities.

Broader Value and Permissionless Innovation

Beyond eduGAIN integration, OpenID protocols provide broader ecosystem value. Real-time data exchange enables immediate credential status verification rather than relying on potentially outdated cached information. This matters particularly for credentials whose status can change rapidly-employment authorisation that might be revoked, professional licenses that might be

suspended, or social security coverage that might lapse. Institutional autonomy is respected through protocols accommodating diverse governance models without requiring centralised control. Legacy system integration is facilitated through clean interfaces enabling modern wallet-based citizen interactions while preserving backend systems institutions' trust.

This layered approach enables permissionless innovation at the service layer where new use cases, credential types, and verification patterns can emerge without requiring central approval. The trust foundation remains standardised and legally robust. The exchange layer provides flexible protocols accommodating innovations without predetermining all possible uses. New credential types can be introduced without waiting for regulatory approval of specific formats. New verification patterns can be implemented to meet specific needs within privacy and user control constraints. New wallet features can be developed by different providers competing on user experience while maintaining interoperability through standard protocols.

This combination of standardised trust with flexible exchange creates infrastructure that is simultaneously reliable enough for critical applications like healthcare and financial services while adaptable enough to accommodate continuous improvement and expansion as requirements change and innovations emerge.

3.3 The Pluralistic Trust Model: EBSI, OpenID and PKI

DC4EU's most significant achievement was delivering the production-ready blueprint for a hybrid trust architecture that respects both technical innovation and sectoral reality. This complex, three-part system of trust emerged as necessary rather than optional for ensuring the EUDI Wallet's scalability and acceptance across the European Union. The architecture accommodates institutions at different points on their digital transformation journeys without forcing all participants to adopt identical approaches regardless of their specific circumstances and constraints.

3.3.1 Foundational Legal Basis and PKI

Every credential issued through the EUDI Wallet ecosystem must meet strict legal requirements ensuring authenticity, integrity, and non-repudiation that enable credentials to carry legal weight equivalent to traditional paper documents bearing official seals and signatures. Public Key Infrastructure and Qualified Electronic Signatures or Seals provide this foundation, refined over decades of experience with electronic transactions requiring legal certainty.

Public Key Infrastructure provides cryptographic security through interconnected mechanisms. Digital signatures prove credential authenticity by demonstrating that credentials were created by claimed issuers and have not been altered since issuance, using asymmetric cryptography where issuers sign credentials with private keys they control exclusively while verifiers check signatures using freely distributable public keys. Certificate chains establish trust anchors by linking issuer certificates back through intermediate authorities to root certificates maintained by nationally recognised certificate authorities, enabling verifiers to confirm that issuers hold valid certificates from trusted sources rather than self-signed certificates anyone could create.

Tamper-evident seals protect data integrity by making any alteration to credential contents immediately detectable through signature verification failures. Even changing a single character causes mathematical verification to fail, alerting verifiers that credentials have been modified after issuance. This provides strong assurance that credentials presented contain exactly the information issuers originally attested to. Non-repudiation ensures issuer accountability by creating mathematical proof that specific issuers created specific credentials, preventing issuers from later claiming they did not issue credentials they actually issued.

The chain of trust extends from specific credentials back through issuer certificates to qualified trust service provider certifications and ultimately to root certificates published on national and EU

trusted lists. A verifier checking a credential can trace this chain mathematically, confirming at each step that certificates are valid, have not expired, and come from entities authorised to participate. The final root certificates anchor the chain in trust lists maintained by national regulatory authorities and aggregated at the European level.

This mutual recognition obligation across all twenty-seven Member States transforms national digital documents into European instruments with automatic legal validity. When an Austrian hospital verifies a digital EHIC issued by Spanish authorities, Austrian law requires recognition of the Spanish qualified seal as legally equivalent to an Austrian government seal. This is mandatory mutual recognition established by EU regulation, not voluntary cooperation. The PKI infrastructure provides the technical mechanism making this legal requirement operationally feasible.

Both the Education and Social Security pilots anchored their implementations in the eIDAS 2.0 Trust Framework and Architecture Reference Framework version 1.5, with PKI providing the cryptographic foundation across the credential lifecycle. Without this PKI foundation, the entire edifice of digital credentials would lack legal weight regardless of other technical sophistications. The pluralistic architecture builds on PKI rather than replacing it, recognizing that legal certainty must precede technical innovation when systems handle credentials with legal and financial consequences.

3.3.2 The Pluralistic Trust Component Summary

The DC4EU pilot demonstrated conclusively that secure, functional deployment requires building on three core, complementary trust components. These are not competing alternatives where choosing one requires rejecting the others, nor redundant layers providing the same capabilities through different mechanisms. They are genuinely complementary components where each contributes distinct capabilities essential for the complete system.

Table 2: The Three Trust Components of the Pluralistic Architecture

Trust Component	Primary Policy Function	DC4EU Application & Goal	Legal/Technical Basis
Public Key Infrastructure (PKI)	Legal Assurance & Non-Repudiation	Guarantees the authenticity and integrity of every credential issued by securing them with Qualified Electronic Signatures/Seals (QES/QSeal) meeting eIDAS requirements. Provides the cryptographic foundation enabling credentials to carry legal weight equivalent to traditional paper documents with official seals.	Mandated by the revised eIDAS Regulation (eIDAS 2.0) for legal enforceability. Decades of operational experience proving reliability at scale across diverse institutional contexts.[2]
European Blockchain Services Infrastructure (EBSI)	Public Sector Trust & Registry Services	Utilised for high-assurance public services, specifically digitising critical Public Body Electronic Attestations of Attributes (Digital Diplomas, Academic Credentials) that root themselves in state authority and governmental oversight.	Compliant with the eIDAS 2.0 Trust Framework. Acts as a Verification Data Registry (VDR) providing capabilities that traditional PKI alone cannot efficiently provide at the European scale, particularly for privacy-preserving verification.[3]

[2] Bauer, G., & Alamillo, I. (2025)

[3] Hilmar, K., Bauer, G., & Beda, K. (2025)

		Provides permanent verifiable records and common governance frameworks across countries and sectors, eliminating need for bilateral agreements between institutions.	
OpenID Protocols & Translation Bridges	Scalability, Interoperability & Privacy	Leveraged as the protocol family to bridge the EUDI Wallet with established academic networks like eduGAIN via VC-aware Service Providers. This demonstrates a realistic migration path for cross-border verification while preserving existing institutional investments and governance models.	Based on OIDC4VCI (issuance) and OIDC4VP (presentation) protocols aligned with the ARF. Utilises a translation layer to convert Wallet presentations into SAML assertions for downstream academic services. Proven at internet scale.[4]

How the Components Work Together

Understanding these components requires examining how they work together in practice. Public Key Infrastructure provides the legal foundation through cryptographic certainty that specific issuers created specific credentials and that those credentials have not been altered. This foundation operates at the base layer, making everything else legally meaningful rather than merely technically impressive. Without PKI, even sophisticated blockchain registries or elegant protocols would produce credentials lacking legal enforceability and cross-border recognition.

The European Blockchain Services Infrastructure operates at the governance and registry layer above the PKI foundation, providing capabilities that traditional PKI alone cannot deliver efficiently at European scale. EBSI establishes common governance frameworks across countries and sectoral schemes, defining clear roles and mechanisms for the complete credential lifecycle from initial authorisation through final revocation. The Verifiable Data Registries enable efficient status checking without requiring verifiers to contact issuers directly for every transaction.

This registry capability carries particular importance for privacy protection. Traditional PKI systems often require verifiers to check certificate revocation lists maintained by issuers or query revocation services that issuers operate, creating privacy vulnerabilities because issuers learn when and where credentials are being verified. EBSI's registry model allows verifiers to check credential status against distributed ledgers without systematically notifying issuers about verification events. This architectural choice directly supports EUDI Wallet privacy requirements by reducing linkability between verification events and preventing issuers from tracking how citizens use their credentials.

OpenID-based protocols and VC-aware service providers operate at the exchange and interoperability layer, providing the communication framework necessary for real-time interaction across the ecosystem while respecting diverse governance models. In the DC4EU education pilots, these protocols, specifically OIDC4VCI for issuance and OIDC4VP for presentation handled the mechanics of how the EUDI Wallet communicates with external systems. Crucially, for the education domain, this layer does not replace existing academic federations. Instead, it utilises VC-aware Service Providers as a practical 'bridge', accepting a verifiable presentation from the EUDI Wallet, validating it against trust anchors, and converting the result into a SAML assertion for downstream services like eduGAIN. This bridge pattern demonstrates how institutions can preserve

[4] Bauer, G., Gabel, H., Hilmar, K., Ilsøe, L., & Kaaber, C. (2025)

their current federation investments and governance models while gradually adopting high-assurance verifiable credentials.

The Architecture Reference Framework serves as the critical governance and semantic layer orchestrating these three components into a coherent system. The ARF demands governance equivalency, semantic alignment, and assurance equivalency across different technical implementations. A credential issued via EBSI must be mutually intelligible with one issued through traditional PKI when both meet equivalent assurance standards. The legal effect of credentials cannot depend on arbitrary technical implementation choices when actual security and verification properties are equivalent.

This orchestration function prevents fragmentation where technically compliant implementations cannot actually interoperate. The ARF ensures that credentials from any conformant source can be verified by any conformant verifier regardless of which specific technical approach was used for issuance. It establishes that verifiers must accept all credential types meeting specified assurance levels rather than arbitrarily limiting acceptance to credentials issued through particular mechanisms.

The architecture is not unnecessarily complex but appropriately complex for the institutional diversity and technical heterogeneity characterizing Europe. Attempts to oversimplify by mandating single approaches would fail to gain institutional acceptance in sectors with substantial existing investments in alternatives. The pluralistic model respects those investments while enabling innovation and establishing common standards where they matter most-in the interfaces between systems and the legal recognition of credentials regardless of their technical provenance.

3.4 Key Technical Achievements

The successful implementation of the three-part trust architecture delivered key technical achievements proving that the system meets the highest standards of EU regulation while providing concrete capabilities that users and institutions require. These achievements extend beyond demonstrating basic functionality to proving that advanced privacy protections, legal compliance, and seamless interoperability can be achieved simultaneously.

“This is not technical complexity for complexity's sake. It is the recognition that you cannot force Italian social security systems built on 20 years of PKI investment to abandon everything overnight. Nor should we prevent Estonian universities from leveraging cutting-edge EBSI capabilities. The architecture respects both realities.”

Operational Validation

Privacy by Design manifests through selective disclosure capabilities built architecturally into credential exchange protocols. Citizens can prove age requirements without revealing exact birth dates, demonstrate enrolment without sharing complete academic transcripts, or establish health insurance coverage without exposing full policy details. GDPR compliance extends beyond surface-level consent dialogues to comprehensive architectural enforcement where the system makes it technically impossible for verifiers to request or receive more information than citizens explicitly approve sharing.

Interoperability demonstrations proved the ecosystem can support multiple wallet implementations without vendor lock-in. The EUDI Wallet Reference Implementation successfully interoperated with DC4EU prototype components across numerous scenarios. Credentials issued through one system were verified by another using different technology stacks, proving that

compliance with open standards enables genuine competition. Offline verification capability enables credentials to be verified without continuous internet connectivity, enhancing both reliability and privacy by preventing real-time issuer notification.

Cross-Border Evidence

The cross-border validation achievements transformed theoretical assertions about mutual recognition into operational reality. Spanish university diplomas were successfully verified by Dutch institutions with no prior bilateral agreements. Polish workers' PDA1 forms were verified by French employers in seconds rather than the weeks traditional processes required. Italian students' enrolment status was recognised by German service providers in real time. These were not laboratory simulations but real credentials with legal significance, real verifiers making consequential decisions, and real citizens whose rights depended on verification succeeding.

The complete set of achievements - privacy by design, GDPR compliance, interoperability across implementations, offline verification enabling resilient operation, and successful cross-border validation with real credentials - settles the question of technical viability. The technology works. The protocols function as specified. The privacy protections are genuine. The legal compliance is verifiable. The cross-border interoperability is demonstrated. What remains for successful deployment is not further technical proof-of-concept work but execution at scale addressing the systemic barriers that Section 5 documents and the policy interventions that Section 6 proposes.

4 Key Pilot Domains

The DC4EU project employed Education and Social Security as critical testing grounds to determine the EUDI Wallet's practical viability under real-world conditions. These domains were not selected for convenience or accessibility but because they represent opposite ends of the institutional spectrum that characterises European public services. The strategic logic was straightforward: if the EUDI Wallet could function successfully across both these dramatically different institutional environments, the architecture could be reasonably assumed capable of handling the full spectrum of European institutional diversity. Conversely, if the wallet worked well in one domain but failed in the other, that failure would signal fundamental gaps in the architecture requiring resolution before widespread deployment.

The contrasts between these domains are profound and multidimensional. Educational institutions typically operate modern IT systems with relatively short refresh cycles, often replacing major systems every five to ten years as technology evolves and institutional needs change. Social Security agencies, by contrast, operate legacy systems where core infrastructure may date back twenty or more years: massive capital investments and accumulated operational knowledge that cannot be abandoned lightly. Educational institutions possess high innovation appetite, frequently positioning themselves as early technology adopters and viewing digital transformation as aligned with their educational mission. Social Security institutions approach change with appropriate caution, recognizing that their systems handle legally binding entitlements where failures can deny citizens critical services like emergency healthcare or proper social security coverage.

Table 3: Contrasting Institutional Environments

Dimension	Education	Social Security
Infrastructure Age	Modern systems (5-10 year cycles)	Legacy systems (20+ years old)
Trust Model	Federated (eduGAIN) or self-contained	Centralised national PKI
Governance	Institutional autonomy	Government mandates
Innovation Appetite	High (early adopters)	Low (risk-averse)
Credential Lifecycle	Long-term (decades)	Dynamic (frequently updated)
Change Approach	Voluntary adoption	Ministerial directives

The governance models differ fundamentally as well. Education operates through federated structures respecting institutional autonomy, with universities maintaining substantial independence even when receiving public funding. Social Security follows centralized national governance where ministries issue directives that agencies must implement rather than suggesting approaches that institutions might voluntarily adopt. Educational credentials typically have long lifecycles measured in decades, with diplomas remaining relevant throughout careers spanning forty or more years. Social Security entitlements change more dynamically, with coverage status potentially shifting monthly as employment situations change and requiring systems capable of updating status information rapidly.

Each domain validated specific pillars of the three-part trust architecture that Section 3 described in detail. The Education and Professional Qualifications work verified successful integration of EBSI infrastructure for issuing Public Body Electronic Attestations of Attributes with OpenID Federation protocols for verification across academic networks. The domain encompassed a comprehensive lifelong learning perspective extending well beyond traditional university degrees to include professional qualifications for regulated professions, vocational training credentials, technical education specialisations, and the emerging category of micro-credentials representing focused

upskilling tied to labour market needs. The long-term nature of educational credentials - diplomas that must remain verifiable for decades after issuance - proved that EBSI's permanent registry model functions as intended even when issuing institutions undergo mergers, name changes, or closure.

The Social Security work verified the complex integration of EUDI Wallets with legally mandated PKI and eIDAS legacy systems that have anchored social security operations for more than two decades. The pilots focused on two high-impact credentials with direct consequences for citizens' fundamental rights: the European Health Insurance Card enabling citizens to access necessary medical treatment while temporarily staying in another Member State, and the Portable Document A1 certifying which country's social security system applies when someone works temporarily abroad. The pilots confirmed that national institutions could retain PKI as their primary trust anchor – that is, respecting massive existing investments and operational knowledge while exploring how EBSI-style registries might enhance future verification capabilities and privacy protection without requiring disruptive infrastructure replacement.

By confirming the feasibility of this pluralistic approach through real credentials carrying legal and financial consequences, DC4EU established the EUDI Wallet's potential to become the foundational digital trust instrument for core cross-border services throughout Europe.

4.1 The Education Domain and Professional Qualifications: Piloting Digital Academic Credentials

The European Education Area's vision of seamless academic mobility has been severely constrained by legacy verification processes that transform credential recognition into bureaucratic ordeals lasting weeks or months. Students accepting positions at foreign universities find themselves waiting for transcripts to be verified through formal channels involving multiple intermediary organizations. Workers with professional qualifications from one Member State face extensive delays obtaining recognition to practice in another, with verification processes that can extend to several months when additional documentation is required or when language translations must be obtained. These delays represent not merely administrative inefficiency but real barriers to the free movement that European integration promises. The EUDI Wallet offers a path beyond these limitations by enabling instant, cryptographically verifiable credential presentation that places control with citizens rather than requiring permission from intermediary bureaucracies for every usage.

The DC4EU Education Work Package approached credentials from a comprehensive lifelong learning perspective extending well beyond traditional higher education. The scope included Higher Education diplomas and degrees from universities representing formal completion of degree programs, Professional Qualifications representing specialised training required for regulated professions such as medical certifications, engineering licenses, and teaching credentials where practitioners must demonstrate completion of specific training to practice legally, Vocational Education and Training credentials attesting to skilled trade competencies acquired through apprenticeships and vocational programs, Technical and Vocational Education and Training covering technical specialisations preparing workers for specific industries, and micro-credentials representing the emerging category of focused upskilling and reskilling tied closely to labour market needs. This breadth reflects the reality that educational credentials serve diverse purposes throughout working lives rather than being concentrated solely in the early career years represented by traditional degree programs.

The Education pilots validated what we term a Dual Issuance Pattern designed to maximise institutional coverage and adoption. Public Body Electronic Attestations of Attributes were issued directly by universities and education ministries using EBSI infrastructure, leveraging the governmental oversight and permanent registry capabilities that EBSI provides for credentials

requiring strong legal anchoring. Simultaneously, non-qualified Trust Service Providers issued Electronic Attestations of Attributes under the hybrid trust model, serving educational institutions not classified as public bodies under their national legal frameworks or institutions preferring not to operate as Qualified Trust Service Providers given the regulatory burden that status entails. Both issuance models proved fully interoperable with the same EUDI Wallet implementations and verification flows, demonstrating that the architectural design successfully accommodates institutional diversity.

This dual approach carries significant policy implications that deserve emphasis. Restricting digital credential issuance solely to public bodies or qualified trust service providers would exclude many legitimate educational institutions from participating in the ecosystem. Private universities, specialised training providers, and professional certification bodies might lack the public body status required for one issuance path while finding the regulatory burden and compliance costs of becoming qualified trust service providers prohibitively expensive for their scale of operations. The dual pattern accommodates this institutional diversity, enabling both public universities issuing through governmental authentic sources and private training providers issuing through accredited but non-qualified mechanisms to participate fully. From the verifier's perspective, the distinction between these issuance paths is invisible - both credential types present with equivalent assurance levels and identical technical verification properties, ensuring that acceptance decisions can be based on actual assurance rather than arbitrary technical preferences.

4.1.1 Core Pilot Success and Technical Viability

The pilot work focused on achieving unified digital trust across three strategic breakthrough areas that together demonstrate the complete transformation from paper-based credential management to citizen-controlled digital credentials. These areas represent not merely technical achievements but fundamental shifts in how credentials are issued, controlled, and verified across European borders.

Digital Diploma Issuance and Ownership: The Sovereignty Shift

Digital diploma issuance and ownership represent the fundamental shift from institutional custody to citizen sovereignty over credentials. Traditional systems position universities as permanent custodians of credentials, with graduates as petitioners requesting official copies whenever verification is needed. This model made sense in a paper-based world where physical documents required secure storage and official copies needed institutional authentication. The EUDI Wallet inverts this relationship entirely by issuing legally valid diplomas directly into citizens' wallets, placing authentic credentials under personal control independent of the issuing institution's continued operation or system availability.

The complete issuance flow validated during piloting demonstrates this transformation concretely through a sequence that completes in minutes rather than the weeks required by traditional processes. A graduating student receives notification that their diploma is ready for issuance into their EUDI Wallet, typically through the university's student portal or a secure message to their authenticated institutional account. The student initiates the request by scanning a QR code presented by the university's credential issuance system or by following a secure link that opens their EUDI Wallet application. The wallet confirms the student's identity using their Personal Identification Data that was established when they first configured the wallet, ensuring the credential will bind to the correct individual through cryptographic linkage rather than merely associating a name with a credential. The university generates the credential containing all relevant information (degree title, field of specialisation, completion date, honours or distinctions earned etc.) and signs it using a qualified electronic seal meeting eIDAS requirements for legal recognition. This seal provides the cryptographic foundation ensuring authenticity and enabling verification by any party with access to the university's published trust anchors. The credential transmits securely

to the wallet via OIDC4VCI protocol with encryption protecting the transmission from interception or tampering. The student receives confirmation through push notification that their diploma is now securely stored and immediately available for presentation to any party requiring proof of their qualification.

The entire process completes in 2 to 3 minutes from the student's perspective, representing a transformation from the seven to fourteen-day wait typical of traditional physical credential delivery through postal services. More significantly, from the moment the credential enters their wallet, the student owns their diploma in a meaningful sense that was impossible with either paper credentials or institution-managed digital records. They can present it for verification anywhere, anytime, even if the issuing university's systems are offline due to maintenance or technical problems, or if the institution has closed, merged with another university, or undergone restructuring that might complicate verification through traditional channels. They can share it selectively, proving their degree status to an employer without revealing their complete academic transcript including courses taken, grades received, or other details irrelevant to employment qualification. They control who sees it and when, maintaining a complete audit trail of all presentations through their wallet's logging functionality. This represents genuine data sovereignty where citizens possess and control their credentials rather than the illusory control that characterises most digital systems where institutions retain ultimate authority over citizen data.

The technical integration work that made this possible demonstrates Europe's commitment to open standards and avoiding vendor lock-in that could undermine digital sovereignty. The WP5 prototype included experimental integration of EBSI infrastructure into the EUDI Wallet Reference Implementation, with all development delivered as open source software across multiple GitHub repositories covering issuer components for credential generation, wallet applications for citizen use, document management systems for institutional integration, and verifier components for credential validation[5]. Any Member State government, university system, or technical provider can download this code without charge, examine its operation to verify security and privacy properties, modify it to meet their specific requirements and institutional contexts, and deploy it in production environments without licensing fees or proprietary restrictions that would create dependencies on commercial vendors. This open approach ensures that European digital infrastructure remains under European control, embodying principles of digital sovereignty rather than depending on closed systems from vendors who might not share European values around privacy protection and user empowerment.

Cross-Border Recognition of Qualifications: Breaking the Mobility Barrier

Cross-border recognition of qualifications addresses one of the most persistent and frustrating barriers to labour mobility within the European Union. Professional qualifications that require years of study and substantial personal investment should theoretically enable practitioners to work throughout Europe, leveraging the single market for professional services. In practice, recognition processes create such friction that many qualified professionals never attempt cross-border moves, effectively fragmenting professional labour markets despite decades of European integration efforts. A nurse qualified in Portugal faces months of uncertainty attempting to obtain recognition in Germany, with processes involving document authentication, credential evaluation by recognition authorities, and often additional requirements whose necessity and legal basis remain unclear. An engineer certified in Poland encounters bureaucratic mazes trying to practice in France, frequently discovering that different French authorities provide contradictory guidance about requirements. These barriers affect not merely individual career prospects but Europe's overall

[5] Fourtounis, G., Mergoupis-Anagnou, F., & Bekakou, A. (2025)

labour market efficiency, economic integration, and ability to address professional shortages by enabling qualified practitioners to work where their skills are most needed.

The traditional qualification recognition process involves extensive document exchange through formal channels, with original certificates often sent by postal mail to recognition authorities who must verify authenticity with issuing institutions, determine equivalence with domestic qualifications according to national frameworks that may not align well with foreign qualification structures, and issue formal recognition decisions that can take weeks or months to produce. The process typically consumes six to eight weeks even when no complications arise, with frequent extensions to several months when additional documentation is required, when translation services must be engaged for documents in languages that recognition authorities cannot process directly, or when issuing institutions are slow to respond to verification requests. The administrative costs fall heavily on both the individual seeking recognition, who may pay several hundred to several thousand euros depending on the qualification type and Member State, and the institutions performing verification, whose staff time devoted to manual processes represents substantial recurring costs.

The EUDI Wallet is meant to transform this multi-month bureaucratic procedure into instant cryptographic verification that completes in seconds. When a Polish engineer presents a digital professional qualification credential to a French recognition authority, the credential contains the complete qualification details structured according to standardised schemas, the cryptographic signature of the issuing Polish institution meeting eIDAS requirements, and references to the trust anchors published on trusted lists enabling verification of the signature's authenticity. The French authority's verification system checks the signature against published trust lists confirming the Polish institution is authorised to issue such qualifications, validates that the credential has not been revoked by checking status information against appropriate registries, and confirms that the issuing institution possesses the accreditation necessary for the specific qualification type. This verification completes in seconds rather than weeks, requires no manual document exchange or postal services, involves zero marginal cost for additional verifications since the cryptographic checking can be repeated indefinitely without consuming resources, and provides higher assurance than traditional paper-based processes that remain vulnerable to document forgery that is difficult to detect without expertise.

Table 4: Cross-Border Recognition Performance Metrics

Metric	Traditional Process	Digital EUDI Wallet	Improvement
Success Rate	Variable (60-80%)	70% (first attempt, no coordination)	Proves feasibility
Verification Time	6-8 weeks	45 seconds	99% time reduction
Administrative Cost	€250-500 per verification	Near-zero marginal cost	95% cost reduction
Coverage	Limited bilateral agreements	12 Member States (pilot phase)	Multilateral trust

Initial deployment across twelve Member States confirmed a 70% success rate for cross-border mutual recognition scenarios on first attempt without any prior coordination or bilateral agreements between participating institutions. Average verification time measured 45 seconds from credential presentation to verification confirmation, compared to six to eight weeks for traditional processes requiring document exchange and institutional coordination. Administrative cost reductions reached ninety-five percent when comparing digital verification requiring only

system operation against paper-based processes consuming substantial staff time for document handling, authentication, and coordination with foreign institutions.

Understanding what this 70% first-attempt success rate means in context is important for accurate interpretation and avoiding either over-optimism or unwarranted pessimism about the results. This represents success across twelve countries with zero prior coordination between institutions, no established bilateral agreements, differences in languages and legal frameworks, diverse institutional structures and technical capabilities, and no advance harmonisation of metadata standards or verification procedures. Achieving this level of interoperability from the starting point proves that the technical foundation is fundamentally sound and that the architectural choices enabling cross-border verification without requiring extensive advance coordination were correct. The remaining thirty percent of transactions that did not succeed on the first attempt did not fail due to technical problems with cryptographic verification, protocol implementation, or system reliability. Instead, failures stemmed from institutional factors that policy interventions can address: unclear national rules about which foreign qualifications must be recognised under which conditions, missing metadata standards preventing verification systems from understanding credential semantics, undefined verification procedures leaving institutions uncertain about how to process digital credentials, and lack of legal guidance about liability for accepting foreign credentials.

"70% success on first attempt across 12 countries with zero prior coordination is remarkable. It proves the technology works. The remaining 30% is exactly what Sections 5 and 6 address - legal clarity, governance, and standardised metadata."

European Learning Model Standardisation: The Semantic Foundation

The European Learning Model provides the semantic foundation enabling cross-border interoperability by establishing standardised credential formats ensuring academic credentials are consistently understood across different systems, languages, and institutional contexts. The fundamental problem it solves is semantic ambiguity: the reality that different education systems use different terminology, different structures, and different conventions for describing qualifications that may be functionally equivalent but appear different when examined superficially. A Spanish university's "Grado" representing a four-year undergraduate program must be immediately understood by a German employer as equivalent to a "Bachelor" degree meeting prerequisites for professional employment, and both must be recognised by a Polish university as meeting admission requirements for master's-level study. Without semantic standardisation enabling this mutual understanding, every credential exchange requires manual interpretation and expert judgment about equivalence, making automation impossible and creating opportunities for misunderstanding that disadvantage both credential holders and organizations attempting to make qualification-based decisions.

The European Learning Model accomplishes this standardisation through several interconnected components working together to enable machine-readable, automatically processable credentials. Common data models for learning achievements define standard structures for representing degree information, course completions, competencies acquired, and assessment results in ways that remain consistent across different issuing institutions and national contexts. Standardised qualification level frameworks provide mappings to the European Qualifications Framework enabling automated determination of whether qualifications meet level requirements for particular purposes, such as university admission or professional licensing. Machine-readable credential formats based on international standards like W3C Verifiable Credentials enable automated processing by verification systems without requiring manual data entry or human interpretation of document contents. Semantic interoperability specifications ensure that credentials issued by one system following ELM standards can be consumed by other systems, with

consistent interpretation of what specific data elements mean regardless of the issuer's location or institutional type.

The European Learning Model has been adopted broadly across European education initiatives extending beyond the EUDI Wallet to include Europass for standardised presentation of qualifications and skills, the European Student Card initiative for student mobility, and various national implementations of digital credential systems. This broad adoption provides consistent semantics across multiple credential types and use cases, reducing fragmentation and ensuring that investments in ELM-compliant systems provide value across diverse scenarios rather than being limited to narrow applications.

4.1.2 The Trust Integration Model: Bridging Academic Identity (eduGAIN)

The DC4EU project's work on education credentials confronted an integration challenge to be solved within reasonable timeframes without forcing disruptive changes on established systems: integrating the EUDI Wallet with eduGAIN, the established global federated identity service that has served research and education communities effectively for more than fifteen years. The eduGAIN federation links over seventy-five national academic identity federations worldwide through coordinated trust frameworks, enabling researchers and students to access resources across institutional and national boundaries using their home institution credentials rather than requiring separate accounts for every resource they need to access. This capability has become essential infrastructure for European research collaboration, with millions of authentication transactions flowing through eduGAIN monthly enabling access to journals, research databases, computing resources, and collaborative tools that modern research depends upon.

The integration challenge stems from fundamental differences between eduGAIN's original design assumptions and the EUDI Wallet's legal and technical requirements imposed by eIDAS regulation. eduGAIN manages what might be termed non-foundational identity suitable for accessing library resources, research databases, and collaborative tools where the consequences of misidentification are relatively contained within academic contexts. When a researcher authenticates to access a journal database, the system needs confidence that they belong to a subscribing institution authorised to access the content, but it does not necessarily require absolute certainty about their legal identity verified against government registries. The authentication assurance levels that eduGAIN typically operates at reflect this purpose, with most federations operating at lower and medium assurance levels appropriate for academic Single Sign-On (SSO) scenarios where convenience and institutional autonomy are valued alongside security.

The EUDI Wallet operates in an entirely different legal and risk environment defined by eIDAS requirements. Under eIDAS regulation, the wallet constitutes an electronic identification means subject to strict legal regimes requiring high assurance about the person presenting credentials, with identity verification meeting standards sufficient for legally binding transactions that could include registering for university admission with legal consequences if fraudulent, proving professional qualifications for employment where incorrect qualifications could create liability, or accessing restricted research data containing personally identifiable information where data protection regulations impose strict access control requirements. The credentials the wallet contains must enable real-time revocation checking ensuring that credentials whose status has changed are not accepted inappropriately, selective disclosure of individual attributes enabling privacy protection through data minimization, and cryptographic verification of authenticity against trusted registries rather than relying solely on federation trust relationships that may not meet legal certainty requirements.

Attempting to force either system to completely abandon its existing model in favour of the other would have failed to gain institutional support for reasons extending beyond mere technical compatibility. eduGAIN federations represent massive investments by universities and research

institutions accumulated over many years of development, deployment, and refinement. The governance model based on federated trust and institutional autonomy reflects deeply held values in academic communities about the independence of universities from governmental control and the collaborative rather than hierarchical nature of research institutions. These values are not merely preferences that can be easily changed but constitute fundamental aspects of academic culture and legal frameworks protecting university autonomy. Demanding that these federations abandon SAML protocols in favour of entirely new approaches would have created resistance that no amount of technical argument about protocol superiority could overcome, as the resistance would be rooted in legitimate concerns about institutional autonomy, governance control, and the disruption costs of wholesale system replacement.

Conversely, the EUDI Wallet cannot compromise on the high-assurance requirements that eIDAS regulation mandates and that use cases like accessing sensitive research data or proving qualifications for professional licensing genuinely require. These are legal obligations and security requirements that cannot be relaxed simply to accommodate existing systems designed for different purposes with lower security requirements. The challenge DC4EU needed to solve was enabling these two systems to work together productively without requiring either side to abandon its fundamental characteristics or compromise its core requirements.

The OpenID Federation Solution: Technical Bridge with Policy Respect

OpenID Federation is a technically robust and privacy-friendly solution that bridges this gap without requiring either side to surrender essential characteristics. OpenID Federation leverages OpenID Connect protocols that have been proven at internet scale across billions of authentication transactions for secure, standardised authentication while enabling dynamic distribution of trust metadata at scale without requiring centralised metadata repositories that would create governance bottlenecks. This combination provides the real-time status checking and cryptographic verification that eIDAS requires for high-assurance credentials while maintaining the federated governance model that makes eduGAIN successful and acceptable to participating institutions that value their autonomy.

The framework supports Selective Disclosure through mechanisms like SD-JWT, enabling users to share minimum necessary information for each transaction rather than surrendering complete credentials whenever any attribute needs verification. This capability aligns perfectly with both GDPR requirements mandating data minimisation and purpose limitation, and the high-assurance needs of the EUDI Wallet that requires precise control over what information is shared for what purposes. The privacy protection operates at the protocol level rather than depending on policy promises, ensuring that implementations cannot easily bypass privacy protections even if they wanted to maximise data collection.

Architecture: The VC-Aware Service Provider as Translation Bridge

The integration architecture introduces what the project termed a VC-aware Service Provider that functions as a translation bridge between the EUDI Wallet's credential model based on verifiable presentations and eduGAIN's SAML-based infrastructure using authentication assertions that have served academic identity management for more than fifteen years. This bridge represents careful architectural design enabling evolutionary transformation rather than disruptive replacement, respecting existing investments while introducing new capabilities.

The bridge accepts verified credential presentations from EUDI Wallet holders using the OIDC4VP protocol with all the privacy protections and user control that protocol provides. It validates those credentials against appropriate trust registries to confirm their authenticity, current validity status, and that they were issued by authorities authorised to make such attestations. The validation process checks cryptographic signatures against published trust anchors, queries revocation

registries to ensure credentials have not been suspended or revoked and verifies that issuers hold appropriate accreditation for the credential types they issued. After successful validation, the bridge extracts relevant attributes from the verified credentials according to the specific information requirements of the relying service, respecting the selective disclosure choices that wallet holders made when approving the credential presentation. These attributes are converted into SAML assertions formatted identically to the assertions that the relying institution has been processing for years through its existing eduGAIN integration, with attribute names, value formats, and metadata conforming to established eduGAIN conventions that existing access control systems can consume without modification.

From the perspective of a university's identity management infrastructure, nothing has changed in how authentication operates. The system receives SAML assertions through the same interfaces it has used for years, with attributes conforming to schemas that existing access control policies reference, and processing occurring through the same software components that handle regular eduGAIN authentications. The university's IT staff do not need retraining on new systems, existing access control policies do not require modification, and troubleshooting procedures that staff have developed through experience remain applicable. From the citizen's perspective, they are using a modern, privacy-preserving EUDI Wallet with selective disclosure enabling them to control exactly what information is shared, user-friendly interfaces explaining what data sharing means in clear language rather than legal terminology, and full audit trails showing where their credentials have been presented. The bridge handles translation invisibly between these two different models, maintaining backward compatibility with existing eduGAIN deployments while enabling forward progress toward wallet-based credentials that provide stronger assurance and better privacy protection than traditional federation models.

This translation bridge pattern provides benefits extending well beyond preserving institutions' SAML infrastructure investments. It enables universities to gradually transition from federation-based identity toward wallet-based credentials at their own pace based on their specific circumstances, institutional priorities, and budget availability. Early adopter institutions can begin issuing credentials directly into EUDI Wallets and building native support for consuming wallet-based presentations directly without waiting for the entire eduGAIN federation to reach consensus on migration timelines, which would likely take many years given the diversity of participating institutions and national contexts. Late adopter institutions can continue relying on traditional federation infrastructure for as long as necessary while benefiting from increased interoperability with wallet-based systems that their students and researchers may be using for non-academic purposes. The bridge remains available as long as institutions need it, providing a safety net that reduces migration risk, while not becoming a permanent dependency preventing eventual direct wallet integration when institutions determine they are ready to move beyond SAML-based federation.[6]

Case Study: High-Assurance Cross-Border Verification in Practice

A concrete scenario illustrates how this integration functions under real-world conditions with actual security requirements and privacy protections operating simultaneously. Consider a Spanish doctoral student at Universitat Rovira i Virgili who needs to access restricted research databases at Utrecht University in the Netherlands. The databases contain personally identifiable research data

[6] The detailed findings and technical architecture that validate this trust model are documented in the publication WP5 eduGAIN: structure, governance and sovereignty in the European academic federated identity ecosystem and the related technical specifications. Also see Den Hertog, P., van Dijk, N., & Wierenga, K. (2025).

drawn from medical studies, making them subject to strict data protection requirements under GDPR and research ethics regulations. Traditional eduGAIN authentication providing basic confirmation of institutional affiliation would be insufficient for access control to such sensitive data: Utrecht University requires eIDAS-level assurance about the researcher's verified identity and explicit confirmation of their research authorisation level appropriate for the data sensitivity involved.

The Challenge: Traditional eduGAIN flows cannot provide the assurance Utrecht requires, but forcing the Spanish university to abandon eduGAIN for an entirely different authentication system would be unacceptable.

The Solution Flow: Three Trust Layers Working Together

Step	Action	Technology	Time
1	Spanish university issues student status as PuB-EAA into EUDI Wallet, including enrolment verification, research authorisation level, and validity period	EBSI + Qualified Seal	One-time setup
2	Utrecht system requests specific attributes via OIDC4VP: "Prove current enrolment status and research authorisation"	OpenID Federation	2 seconds
3	Student's wallet displays request in clear language: "Utrecht University requests: Enrolment status, Research authorisation level, Validity dates"	Wallet UI + Selective Disclosure	5 seconds
4	Student reviews what will be shared (NOT grades, NOT course history, NOT home address) and approves with biometric/PIN	User consent	3 seconds
5	Wallet creates Verifiable Presentation containing only approved attributes	Selective Disclosure Protocol	2 seconds
6	Utrecht verifies credential signature and checks status against Spanish VDR - Spanish university receives NO notification	EBSI Registry + PKI Signature	3 seconds
7	Access granted to restricted research database	System integration	Instant
Total	**Complete high-assurance verification and access**	**All three trust layers working together**	**< 60 seconds**

The Outcome and Significance:

The student gains access to the restricted research database in under sixty seconds from initial request to final authorisation, compared to the weeks that traditional verification through formal channels between universities would require, involving document exchange, manual verification of enrolment and research ethics approval, and coordination between international offices. Utrecht University has legal certainty of the student's enrolment status and research authorisation meeting the assurance requirements of GDPR compliance for sensitive data access demands. The Spanish university receives no notification that this verification occurred, preserving the student's privacy by preventing the university from tracking which external resources the student accesses and how frequently, information that could reveal sensitive details about research interests or career planning. The student shared only the information strictly necessary for the access decision (enrolment status and research authorisation level), without revealing grades, complete course history, home address, or any other attributes irrelevant to Utrecht's legitimate access control needs.

This scenario demonstrates capabilities that were genuinely impossible with pre-EUDI systems given the tension between the assurance requirements for accessing sensitive data and the relatively low assurance that traditional academic federation provides. Achieving eIDAS-level assurance for accessing sensitive research data would have required weeks of manual verification through formal channels, with universities exchanging official letters confirming enrolment and

authorisation, research ethics committees providing documentation of approval, and administrative staff coordinating the verification through procedures that have no standardised format or timeline. Alternatively, institutions might have accepted lower assurance levels that did not adequately meet data protection requirements for the sensitivity of data involved, creating legal risks for both the providing institution that could face sanctions for inadequate access controls and researchers who might inadvertently violate data protection regulations. OpenID Federation integration with the EUDI Wallet makes the process instant, provides the high assurance that legal and ethical requirements demand, and preserves privacy through architectural design rather than merely through policy promises that might not be honoured.

4.2 The Social Security Domain: EHIC and PDA1

Digital Identity Intersects with Fundamental Rights

The social security domain represents where digital identity technology directly intersects with citizens' fundamental rights and welfare in ways that extend far beyond administrative convenience or efficiency gains. The credentials tested in this domain are not optional enhancements to user experience but essential entitlements that can literally mean the difference between receiving healthcare abroad or facing denial of service with potentially health-threatening consequences, or between working legally across borders with proper social security coverage or facing penalties, double taxation, and improper deductions that affect workers' livelihoods and retirement security. The stakes for getting implementation right extend beyond technical success metrics to questions of social solidarity that lie at the heart of European integration and the practical meaning of European citizenship for millions of people who travel, work, or study across borders.

DC4EU focused on two credential types that European regulation recognises as Public Body Electronic Attestations of Attributes, issued by authentic sources within public sector organisations. While distinct from Qualified Electronic Attestations of Attributes in legal form and supervisory regime, these credentials demonstrated high technical assurance and operational reliability appropriate to their sectoral legal context.

Their legal characteristics derive from public-sector issuance and authentic source governance rather than from qualified trust service status. As a result, they benefit from specific recognition and acceptance obligations under Union and sectoral law, without carrying the automatic legal presumptions associated with qualified trust services..

Table 5: Social Security Credentials

Credential	Purpose	Traditional Problems	Digital Solution
European Health Insurance Card (EHIC)	Grants EU citizens assured access to necessary medical treatment across all Member States during temporary stays	Physical cards are frequently lost, damaged, or forgotten when traveling; no mechanism for real-time validity checking creates uncertainty; fraud is difficult to detect without contacting issuing countries	Digital credential always available in phone that citizens carry constantly; instant cryptographic verification provides certainty; real-time status checking distinguishes active coverage from expired entitlements
Portable Document A1 (PDA1)	Certifies which country's social security system applies when someone works temporarily abroad; prevents double contributions to both	Paper forms require 3-6 weeks to obtain through bureaucratic processes; verification requires contacting issuing country creating delays; fraudulent	Digital credential issued within 24 hours through streamlined process; instant cryptographic verification eliminates need for cross-border

	home and host country systems	documents difficult to detect	coordination; authenticity guaranteed through qualified seals

Under the EU Social Security Coordination framework, the European Health Insurance Card (EHIC) enables insured persons to access medically necessary healthcare during temporary stays in another Member State under the same conditions and at the same cost as persons insured in the host country. The EHIC covers both emergency treatment and care that cannot reasonably be deferred until return to the competent Member State. It supports reimbursement and cost-settlement mechanisms between national institutions in accordance with the host country's procedures and tariffs, rather than conferring a separate or autonomous healthcare entitlement. Over decades of use, the physical EHIC has become a widely recognised and trusted instrument of European social rights, carried by millions of citizens travelling within the Union for tourism, work, study, or family reasons.

Digitisation of the EHIC addresses well-documented operational shortcomings inherent to physical cards. Loss, accidental damage, or expiry of cards occurs regularly and creates uncertainty for both patients and healthcare providers. Physical cards cannot support real-time verification of entitlement status and may be presented even after insurance coverage has changed due to employment or residency transitions. Digital EHIC credentials enable instant verification of authenticity and current validity, reducing the risk of incorrect assumptions about coverage and preventing downstream reimbursement disputes between institutions. This improves administrative efficiency while strengthening legal certainty for patients and providers alike.

A complementary but distinct function within social security coordination is served by the Portable Document A1 (PDA1). Under Regulations (EC) No 883/2004 and 987/2009, the A1 certifies which Member State's social security legislation applies to a person temporarily working or self-employed in another Member State. The document is a legally required proof for posted workers and certain self-employed persons and is essential to prevent double contributions and conflicting claims by multiple national systems. In this context, the A1 is not a convenience instrument but a prerequisite for lawful cross-border work and for safeguarding workers' social security rights.

Paper-based A1 processes have long been recognised as a bottleneck to lawful labour mobility. Issuance typically requires several weeks, during which employment may not legally commence. Employers and workers face legal and financial uncertainty, while labour inspectors and social security institutions encounter difficulties verifying authenticity and validity across borders. Verification requests often rely on slow, manual exchanges between institutions, and fraudulent or improperly issued documents are difficult to detect systematically. These weaknesses undermine both enforcement and trust in the coordination system.

Digital PDA1 credentials directly address these challenges. Electronic issuance enables significantly shorter processing times, allowing workers to receive proof of applicable legislation before or immediately upon commencing cross-border work. Verifiers—including employers, labour inspectors, and competent institutions—can confirm authenticity and validity through cryptographic verification against trusted national and European trust infrastructures, rather than through ad hoc institutional correspondence. This improves enforcement effectiveness, reduces administrative burden, and strengthens protection against fraud.

Institutional Continuity and Evolutionary Modernisation

DC4EU social security pilots demonstrated that EHIC and PDA1 can be issued and verified as Public Body Electronic Attestations of Attributes, achieving high technical assurance while deliberately preserving established national issuance, validation, and revocation processes. These processes are

deeply embedded in long-standing national PKI and eIDAS-based infrastructures that social security institutions have operated reliably for decades. This approach reflects institutional reality: social security systems manage mission-critical entitlements affecting millions of citizens, where system failure would have immediate legal, financial, and social consequences.

Rather than replacing proven infrastructures, the EUDI Wallet layer adds value by enabling citizens to carry credentials digitally, supporting selective disclosure of only the information required for a specific interaction, and enabling real-time validity checking without direct contact with issuing institutions. Innovation therefore occurs through the evolutionary enhancement of trusted, operational systems, rather than through the disruptive replacement of infrastructures that already function reliably at scale.

At the same time, the pilots assessed how alternative trust mechanisms—such as registry-based approaches—could be considered in the future alongside existing PKI-based models. In practice, Social Security use cases relied on revocation and status lists, Union-level metadata structures, and Member State–specific metadata reflecting local policy requirements. This approach preserves institutional continuity while leaving room for the adoption of additional technologies where legal clarity, organisational readiness, and risk management conditions permit..

4.2.1 Implementation and Workflow

The piloting phase successfully demonstrated the complete, end-to-end user workflow for issuing and verifying Public Body Electronic Attestations of Attributes, using the EHIC as the primary proof-of-concept while also validating the more complex PDA1 scenarios involving employment verification and coordination between home and host country social security systems. The standardised user journey follows four distinct, secure steps that together transform credential management from institution-centric processes where citizens are passive recipients to citizen-centric processes where individuals control their credentials and determine how they are used.

Step 1: Request and Identity Binding

The request and identity binding phase represents the first citizen interaction with the digital credential system and establishes the foundation for subsequent security through verified identity linkage. Traditional processes for obtaining an EHIC imposed substantial friction through requirements that citizens visit social security offices in person or submit paper applications by post, provide paper documentation proving their eligibility for coverage often including employment letters or insurance policy documents, wait seven to fourteen days for processing while applications moved through bureaucratic workflows, and receive the physical card through postal delivery that could be delayed or lost in transit. This process imposed particular hardship for citizens living far from social security offices who might need to take time off work for the visit, for people needing cards urgently before unplanned travel, and for anyone who had lost a card while travelling and needed replacement while away from home.

Table 6: Request and Identity Binding Comparison

Traditional Process	Digital EUDI Wallet Process	Impact
Visit social security office in person or submit paper application	Open national social security mobile app or web portal	Eliminates travel requirement
Provide paper documentation proving eligibility	Authenticate using existing national eID credentials	Leverages existing identity infrastructure
Wait 7-14 days for processing	Request digital EHIC through simple interface	Immediate processing
Receive physical card by postal delivery	Identity automatically bound using PID; credential delivered to wallet	Eliminates delivery delays and loss risk
Total time: 7-14+ days	**Total time: 2-3 minutes**	**99% time reduction**

The digital process reduces this multi-day ordeal to minutes through streamlined workflows leveraging existing infrastructure. Citizens open their national social security mobile application or web portal, systems they already use for checking coverage status, viewing contribution history, or accessing other social security services. They authenticate using existing credentials - typically their national electronic identification system that they already use for other government services, eliminating the need to manage separate credentials for social security access. They request issuance of a digital EHIC through a simple interface requiring no technical expertise, just indicating they need the credential added to their wallet. The system automatically binds the credential to the citizen's verified identity using their Personal Identification Data from their EUDI Wallet, ensuring the credential cannot be fraudulently transferred to another person or used by someone other than its rightful holder. This identity binding provides security equivalent to physical possession of a card that includes a photograph but achieved through cryptographic linkage rather than visual comparison of photos that can be imprecise and that some physical cards omit entirely.

The entire request and identity binding process completes in two to three minutes from the citizen's perspective, representing a ninety-nine percent reduction in time compared to traditional processes and transforming credential acquisition from a task requiring planning and dedicated time into something that can be accomplished spontaneously when needed. More importantly, the process can occur from anywhere with internet access rather than requiring physical presence at specific locations during specific business hours, dramatically improving accessibility for people with mobility limitations, work schedules conflicting with office hours, or residence in areas distant from social security offices.

Step 2: Secure Storage

Secure storage addresses the fundamental question of where credentials reside and who controls access to them, with implications for both security and sovereignty over personal data. The social security authority generates the EHIC as a Public Body Electronic Attestation of Attributes containing the policy number that billing systems use to identify coverage, coverage dates establishing the validity period during which the card remains effective, issuing country information enabling proper routing of reimbursement claims, and other necessary information that healthcare providers and billing systems require for processing covered treatment. This credential receives cryptographic signing using a qualified electronic seal meeting eIDAS requirements, providing the legal certainty and non-repudiation properties that enable the digital credential to carry the same legal weight as the physical card bearing official seals and signatures. The sealed credential transmits securely to the citizen's EUDI Wallet via OIDC4VCI protocol, with the transmission itself protected by encryption preventing interception or tampering by malicious actors who might attempt to capture credentials during transit.

Once received, the credential is stored locally in the citizen's wallet with encrypted protection ensuring that device theft or unauthorised physical access cannot expose the credential contents to someone who should not have them. The wallet application provides user-controlled backup to secure cloud storage with encryption keys that only the citizen possesses, enabling credential recovery if the primary device is lost, stolen, or damaged beyond repair. Citizens receive push notification through their device's notification system that their digital EHIC is ready, can open the wallet application to verify its presence and review its contents, and have immediate confidence that the credential is available for use whenever needed without depending on whether they remembered to pack a physical card or whether that card is still in their wallet rather than being left somewhere.

This storage model fundamentally differs from traditional approaches where institutions maintain custody of credentials and citizens must request access when needed, either by applying for official copies or by proving possession of physical credentials that institutions issued previously. With the EUDI Wallet, citizens own their credentials in a meaningful sense that was impossible with institutional custody models, possessing authentic credentials under their personal control that they can present independently of whether issuing institutions are available, cooperative, or even still in existence.

Step 3: Point of Use Presentation

Point of use presentation occurs when citizens actually need to use their credentials for real purposes - in the EHIC case, when receiving medical treatment while traveling in another Member State. Traditional processes required presenting the physical card to healthcare providers, with medical staff or administrative personnel manually recording details by copying information from the card into their systems. This manual process proved time-consuming, error-prone with data entry mistakes occurring in fifteen to twenty percent of cases according to healthcare facility surveys and created uncertainty about whether the card remained valid or had been cancelled due to changes in insurance status that the healthcare provider had no practical way to verify in real-time.

Table 7: Point of Use Presentation Comparison

Traditional Process	Digital Process	User Experience
Present physical card (85% success if remembered)	Healthcare provider displays QR code or requests NFC tap	No dependency on remembering physical card
Staff manually records details (2+ minutes)	Wallet prompts: "Share EHIC with [Hospital Name]?"	Clear, simple question
Uncertain if card is valid/expired	Shows exactly what data will be shared: ✓ Active coverage status ✓ Policy number ✓ Coverage dates ✗ NOT home address ✗ NOT other credentials	Complete transparency and control
Potential for data entry errors (15-20% error rate)	Citizen approves with biometric or PIN	Secure, quick authorisation
Time: 2+ minutes, 80% overall success	**Time: 10-15 seconds, near 100% success**	**Faster and more reliable**

The digital process transforms this interaction into a rapid, automated exchange that completes in seconds rather than minutes while providing higher assurance and better privacy protection. The

healthcare provider displays a QR code at their reception desk or examination room using their existing computer systems with minimal modification, or requests an NFC tap from the citizen's mobile device if both devices support that capability. The citizen's EUDI Wallet detects the verification request and prompts with a clear, understandable question: "Share EHIC with [Hospital Name]?" where the hospital name comes from the verification request and displays to the citizen so they can confirm they are sharing with the intended party rather than with a fraudulent system that might be attempting to collect credentials. The wallet shows exactly what data will be shared if the citizen approves, displaying in simple language that active health coverage status will be shared indicating yes or no, policy number will be provided for billing purposes, and coverage validity dates will be shared establishing the time period during which coverage is active. Critically, the interface also shows what will not be shared - not the citizen's home address unless that is specifically required by the healthcare provider's systems and justified for the medical purpose, not other credentials the wallet might contain like driver's licenses or diplomas, and not unnecessary personal information beyond what coverage verification requires.

The citizen approves sharing using biometric authentication like fingerprint or face recognition that their device supports, or by entering their wallet PIN if biometric authentication is unavailable or if they prefer PIN-based authorisation. The entire presentation process completes in ten to fifteen seconds from displaying the QR code to receiving verification confirmation, substantially faster than manually recording information from a physical card while providing higher assurance that the credential is authentic and current rather than potentially expired or fraudulent. The success rate approaches one hundred percent because citizens cannot forget their mobile phones with the same frequency they forget specific cards, credentials cannot become illegibly damaged in ways that prevent machine reading, and verification does not depend on staff correctly transcribing information from cards to computer systems.

Step 4: Real-Time Verification

Real-time verification represents the final step where the healthcare provider's system confirms the credential's authenticity and current validity, providing the assurance necessary for confident treatment provision and proper billing. The verifier receives a Verifiable Presentation containing only the EHIC attributes the citizen approved for sharing, formatted according to standard protocols that verification systems can process automatically without requiring custom integration for each credential type or issuing country. The presentation includes cryptographic proof of authenticity through the qualified electronic seal that the issuing social security authority applied when generating the credential, enabling mathematical verification that confirms the credential originated from the claimed issuer and has not been altered since issuance.

The verification system performs multiple checks operating in parallel to provide comprehensive assurance. It verifies the cryptographic signature on the presentation itself, confirming it came from the citizen's wallet and was not modified during transmission. It extracts the EHIC credential from the presentation and verifies the qualified seal on the credential against Spain's published trust anchors available through EU trusted lists, confirming the signature matches what would be expected from Spanish social security authorities. It checks the credential status against appropriate registries, confirming the credential has not been revoked or suspended due to changes in coverage status. It validates that all timestamps are appropriate, ensuring the credential was issued before the current date, remains within its stated validity period, and that the presentation occurred recently enough to prevent replay attacks using old presentations that might have been captured by malicious actors.

All these verification steps are completed within approximately thirteen seconds from the moment the citizen scans the QR code to the moment the healthcare provider's system displays "Coverage Verified" with a confirmation indicator that medical staff can understand without technical expertise. The emergency department staff or primary care provider can proceed with treatment

confident in the patient's coverage status and with proper documentation for subsequent reimbursement claims through established cross-border healthcare arrangements. The verification provides legal certainty backed by cryptographic proof rather than merely trust-based assumptions that physical cards require, where staff must assume the card is genuine and current without having practical means to verify those assumptions in real-time.

What the verification process explicitly does not do matters as much as what it accomplishes, particularly for privacy protection. The healthcare provider does not gain access to the citizen's full medical history that might be stored in other systems or credentials. They do not receive information about other credentials stored in the wallet that are irrelevant to the healthcare scenario. They do not obtain unnecessary personal data beyond what EHIC verification specifically requires for coverage determination and billing. Most importantly for privacy, the verification completes without systematically notifying the issuing Social Security authority that verification occurred, preventing authorities from accumulating detailed records of where citizens seek treatment, how often they travel, and what their patterns of healthcare usage reveal about their personal lives and health conditions. This represents Privacy by Design operating at the architectural level, where the system makes surveillance difficult through its fundamental structure rather than merely promising privacy protections through policies that might not be honoured or legal restrictions that could change.

Concrete Example 1: The PDA1 Success Story - Polish Worker in France[7]

The Situation: A Polish construction worker receives an offer for a three-month temporary assignment with a French construction company involved in a major infrastructure project. In practice, the French employer requires confirmation of applicable social security legislation before allowing work to commence, as the absence of an A1 certificate exposes employers to significant legal and financial risk. Without an A1, French authorities may presume that French social security law applies, potentially resulting in retroactive contributions, penalties, and sanctions for the employer, while the worker risks conflicting claims from both Polish and French systems.

Traditional Timeline and Its Consequences: Under traditional procedures, the worker applies to Poland's social security institution (ZUS) in advance of the planned start date, submitting employment documentation, proof of ongoing Polish social security coverage, and supporting materials that may require translation depending on language and content. The application proceeds through administrative verification, assessment of posting conditions under Regulation (EC) No 883/2004, document issuance, and delivery, often by post. In many cases, this process takes several weeks—and frequently three to six weeks—during which employers are reluctant to allow work to begin.

For workers who must relocate, secure housing, and arrange travel, these delays create uncertainty and financial strain. For employers operating under tight project timelines, uncertainty over social security compliance may lead to the engagement of alternative workers who can begin immediately, causing the posting opportunity to be lost altogether.

[7] Hilmar, K., Bauer, G., & Beda, K. (2025)

Digital Journey and Transformation:

Timeline	Action	Result	Impact
Week 0 – Before Leaving Poland	Worker requests digital PDA1 from ZUS via mobile application, submitting employment contract electronically	ZUS performs automated checks of contribution status and posting criteria, with manual review where required	Processing has been reduced from weeks to hours or a small number of days in straightforward cases
	ZUS issues PDA1 as a **Public Body Electronic Attestation of Attributes**, sealed using high-assurance electronic sealing compliant with eIDAS	Credential is securely transmitted to the worker's EUDI Wallet	Immediate digital availability once issued
	The worker receives confirmation notification	Typical elapsed time: up to 24–48 hours in uncomplicated cases	A worker can plan relocation with greater certainty
Week 1 – Arrival in France	French employer initiates verification via QR code or standard wallet interaction	Worker presents digital PDA1 with selective disclosure	No language barriers; standardised process
	Employer's system cryptographically verifies authenticity and validity against trusted Polish trust information	Verification establishes a strong presumption of applicable Polish social security legislation	No routine need to contact Polish authorities
	Employment contract finalised and work begins	Elapsed verification time: seconds to minutes	No lost opportunity or income
Ongoing – Compliance and Enforcement	French labour inspectors verify PDA1 during routine inspections using mobile devices	Authenticity and current validity confirmed at inspection time	More efficient enforcement
	Status changes (e.g. end of posting) recorded by issuing institution	Updated status becomes verifiable when recorded	Reduces risk of improper coverage
	Digital record retained	No paper storage or manual record-keeping	Reduced administrative burden

The Transformation and Broader Implications:

The digital process substantially shortens the time between job offer and lawful commencement of work. In straightforward cases, workers can begin employment weeks earlier than under traditional paper-based procedures, avoiding income loss caused by administrative delays and enabling acceptance of opportunities that would otherwise be infeasible without extensive advance planning. For employers, immediate access to cryptographically verifiable documentation significantly reduces compliance risk at the start of employment and eliminates the need for manual tracking of pending A1 applications or repeated follow-up with foreign social security institutions, thereby lowering administrative overhead for human resources functions.

For host-country authorities, digital credentials enable more effective and timely enforcement. Labour inspectors can verify the authenticity and current validity of PDA1 documentation during routine worksite inspections using standardised digital tools, without relying on paper documents that may be unavailable, outdated, or difficult to authenticate. At the same time, issuing institutions in the home Member State retain full authority over coverage determinations. When changes in circumstances are recorded—such as the end of a posting or a change in employment status—updated information becomes available for subsequent verification, reducing reliance on delayed institutional notifications and mitigating the risk of improper coverage.

Beyond efficiency gains, the most significant impact lies in expanding the practical scope of lawful cross-border employment. Traditional timelines effectively exclude short-term assignments from participation in the coordinated social security framework, as opportunities lasting only a few weeks cannot accommodate documentation processes that themselves take several weeks. Digital issuance and verification make such short-duration postings realistically accessible, increasing

labour market flexibility while preserving legal certainty and social protection. This enables workers to respond to cross-border demand as it arises and allows employers to fill short-term needs without compromising compliance, reinforcing the effective functioning of the internal market for labour.

Concrete Example 2: Healthcare Provider Feedback - Digital EHIC[8]

Survey results from healthcare providers participating in pilot testing provide strong empirical evidence of institutional demand for digital social security coordination credentials. This demand extends beyond technological enthusiasm or compliance with regulatory mandates and reflects the assessments of professionals directly responsible for operational use. Respondents included emergency department staff managing urgent cases, billing departments handling cross-border reimbursement under Regulation (EC) No 883/2004, primary care providers treating temporarily resident patients, and coordinators responsible for organising cross-border healthcare in accordance with Regulation (EC) No 987/2009.

These respondents are well positioned to evaluate whether digital verification mechanisms address concrete operational challenges inherent in the current coordination framework, rather than introducing additional complexity into already constrained clinical and administrative workflows.

Survey Question: "How important is the introduction of electronic and real-time verification for the EHIC to your institution?"

Quantitative Results:

- **90%** of respondents (healthcare facilities/administrators) rated it as highly important or essential
- **8%** rated it as moderately important
- **2%** rated it as low importance

This overwhelming support comes from healthcare professionals and administrators who can evaluate whether proposed solutions address real problems they face daily or merely add complexity to already challenging workflows. The enthusiasm is not driven by technological novelty but by recognition that current processes create genuine problems that digital verification could solve.

Qualitative Feedback Themes:

Theme	Representative Quote	Context
Fraud Prevention	*"Currently we have no way to verify if an EHIC card is genuine without calling the issuing country - which we never do in emergencies. Digital verification would eliminate fraud risk while maintaining rapid treatment."*	Emergency department administrator, Italy
Administrative Efficiency	*"Manual data entry from physical cards creates errors in 15-20% of cases, leading to reimbursement delays that can take months to resolve. Digital credentials integrating directly with our systems would eliminate these errors."*	Hospital billing department, Germany
Patient Care Quality	*"Real-time verification means we can provide treatment immediately with confidence in coverage. No more uncomfortable conversations asking patients to call their home country's insurance helpline while they're sitting in our waiting room."*	Primary care provider, Spain

[8] Bauer, G., Hilmar, K., Damdinbazar, K., Ilsøe, L., Friedl, P., Alamillo-Domingo, I., & Kaaber, C. (2025)

Cross-Border Coordination	*"For planned treatment abroad under the directive, the ability to verify coverage status before the patient travels would transform administrative coordination and prevent situations where patients arrive for procedures only to discover coverage problems."*	Cross-border healthcare coordinator, Belgium

Verifier-Side Uncertainty, Onboarding Risk, and Mitigation Mechanisms

Despite the strong institutional demand identified, DC4EU piloting demonstrated that acceptance, onboarding, and operational integration at the verifier level remain the principal sources of uncertainty and deployment risk, particularly for the EHIC use case. Unlike PDA1 verification—which is typically performed by a comparatively limited set of employers, labour inspectors, and administrative bodies—EHIC verification must be supported across a highly fragmented verifier landscape that includes hospitals, emergency departments, primary care practices, billing intermediaries, and regional health authorities. In addition, the EHIC is routinely used in practice beyond the strict scope of formal social security coordination, serving as a commonly accepted proof of health insurance coverage in administrative admission procedures and in ancillary services where individuals are required to demonstrate insurance status before registration or service access. Many of these actors operate under tight budgetary, staffing, and reliability constraints, and are therefore highly sensitive to implementation risk.

Pilot experience showed that the dominant barriers for verifiers are not conceptual resistance or lack of perceived value, but practical feasibility: uncertainty about integration cost, disruption of clinical or billing workflows, liability exposure during transition, and the absence of ready-to-use technical components. In emergency care settings in particular, even modest increases in system complexity or failure risk are viewed as unacceptable.

DC4EU piloting also generated concrete evidence that these risks can be substantially reduced through targeted design and support measures. In particular, the provision of open-source reference implementations, shared development of core components, and reuse of common libraries significantly lowered the entry threshold for verifier onboarding. Where healthcare providers and system vendors could rely on tested, openly available components rather than developing bespoke solutions, integration effort and perceived technical risk were markedly reduced.

In addition, the use of verifier proxies—intermediate components that handle credential verification on behalf of multiple institutions—proved effective in addressing both technical and organisational constraints. Such proxies allow individual healthcare providers to integrate digital verification without embedding full cryptographic and trust-resolution logic into their own systems, reducing complexity while preserving legal and technical assurance. This model is particularly relevant for smaller providers and legacy hospital information systems that cannot be rapidly adapted.

Beyond technical tooling, DC4EU evidence indicates that positive incentives play a critical role in adoption. Verifiers were more willing to engage when digital EHIC verification demonstrably accelerated existing processes, reduced manual work, improved data quality, or enabled greater automation in billing and coordination workflows. In these cases, digital verification was not perceived as an additional compliance obligation, but as a mechanism for process improvement and cost reduction within existing legal frameworks.

Harmonisation with PDA1 Experience

These findings are consistent with, but more pronounced than, observations from digital PDA1 pilots. In both cases, the legal value of digital Public Body Electronic Attestations of Attributes depends on widespread verifier capability to accept and validate them reliably. For PDA1, the

narrower and more specialised verifier population makes onboarding more tractable. For EHIC, the scale and diversity of verifiers magnify the importance of shared infrastructure, open-source components, verifier proxies, and incentive-aligned process redesign.

Taken together, DC4EU results indicate that successful deployment of digital EHIC and PDA1 credentials requires more than legal enablement and technical specification. It depends on an ecosystem strategy that actively reduces verifier-side risk through shared development, reusable artefacts, intermediary services, and incentives aligned with operational benefits. Without these measures, uncertainty at the verifier level is likely to translate into uneven adoption, undermining the cross-border effectiveness of the social security coordination framework despite clear institutional demand

4.3 Architectural Proof: The Hybrid Trust Model in Practice

Synthesising Three Trust Layers into One Seamless Transaction

The preceding sections have shown that the Education pilots primarily employed EBSI-based trust registries and OpenID Federation models, while the Social Security pilots relied on established national PKI infrastructures, complemented by revocation and status lists for verification, Union-level metadata structures, and additional Member State–specific metadata reflecting local policy requirements. The pilots also demonstrated the ability to combine multiple attestations within a single presentation, for example by jointly presenting base identity data and an EHIC credential, allowing verifiers to assess both the holder's identity and entitlement in one coherent interaction. This section demonstrates how these distinct trust components can be synthesised within a single functional transaction, providing architectural evidence that pluralistic trust coexistence operates not merely as a theoretical construct but as an operational reality. The transaction reflects real-world conditions involving actual citizens, authentic credentials with legal and financial implications, and time-critical scenarios in which failure would have immediate and tangible consequences..

Demonstration: Cross-Border Social Security (Digital EHIC)

The Scenario and Its Significance:

Maria, a Spanish citizen insured under the Spanish social security system, is on holiday in Austria on a skiing trip when she develops acute symptoms—high fever, respiratory distress, and chest pain—requiring immediate medical attention. Upon arrival at the emergency department of an Austrian hospital, healthcare providers must proceed with treatment in accordance with national medical rules, while also determining whether Maria is insured in another Member State for the purposes of social security coordination under Regulation (EC) No 883/2004. This determination is necessary to ensure that care provided as medically necessary during a temporary stay can be correctly attributed and reimbursed between competent institutions.

Maria presents her digital European Health Insurance Card (EHIC) via her EUDI Wallet to the hospital's registration system. The EHIC serves as proof that she is insured under Spanish legislation and therefore eligible for coordination of benefits, enabling the Austrian provider to apply the appropriate administrative procedures for cross-border reimbursement without delaying treatment. Where required, the presentation may combine the EHIC with base identity data to support reliable identification of the patient for administrative purposes.

This scenario is deliberately routine. Comparable situations arise daily across the Union as tourists, students, temporary workers, and other mobile citizens require unplanned medical care during temporary stays in another Member State. Precisely because such cases are common, they provide a stringent test of the coordination mechanisms established by Union law. The interaction must function reliably under time pressure, support accurate verification for coordination purposes, and

provide sufficient assurance for healthcare providers and institutions to act with confidence. The scenario therefore illustrates how digital EHIC verification within the EUDI Wallet framework can support the effective operation of social security coordination in real-world conditions, without altering the substantive rights or obligations defined by the coordination regulations.

Layer 1: Foundational Assurance (Traditional PKI)

What Happens During Original Issuance (Long before Maria requires emergency care)

When Spain's competent social security or health authority issues Maria's digital European Health Insurance Card (EHIC) as a Public Body Electronic Attestation of Attributes, the process begins with authoritative identity and entitlement verification. Maria's identity is verified against national population and civil registries, ensuring that the credential is bound to a legally established person rather than to self-declared attributes. Her entitlement is confirmed by checking coverage status in Spain's social security and health insurance systems, verifying that she is insured under Spanish legislation and eligible for EHIC issuance under Regulation (EC) No 883/2004.

Once these checks are completed, the EHIC credential is cryptographically sealed using high-assurance electronic sealing based on Spain's national PKI infrastructure, operated in accordance with eIDAS requirements for public sector trust services. The seal binds the credential contents to the issuing authority and protects integrity and authenticity over time. Verification of the seal relies on certificate chains anchored in trusted national certification authorities that are made available to other Member States through established trust distribution mechanisms.

This PKI-based sealing provides the foundational assurance layer that makes the credential legally and operationally meaningful across borders. Austrian institutions do not need to rely on institutional familiarity with Spanish systems or bilateral arrangements. They rely instead on cryptographic verification of the issuing authority's seal, supported by Union law obligations to recognise compliant electronic attestations issued by public bodies of other Member States.

Why This Legal–Technical Foundation Matters

Without this PKI foundation, cross-border acceptance would depend on discretionary trust decisions by each verifier. Historically, such discretion led to additional checks, delays, or outright refusal of foreign documentation. The eIDAS framework removes this uncertainty by establishing a common legal and technical basis for recognising electronic attestations issued by public authorities, regardless of national origin.

The Austrian hospital does not need to "trust" Maria personally, nor to make a subjective judgment about the quality of Spanish administrative systems. Trust is anchored in mathematical verification of cryptographic seals and in the legal obligation to accept conformant foreign public-sector attestations. This enables automated verification decisions based on objective criteria rather than human judgment under time pressure.

Layer 2: Validity and Status Verification (PKI Status Lists and Metadata)

What Happens During Real-Time Verification

At the moment Maria presents her digital EHIC in Austria, the hospital's verification system must confirm not only that the credential was validly issued, but also that it remains valid at the time of use. This is essential because EHIC entitlement can change if, for example, a person transfers residence, changes insurance regime, or ceases to be insured under the competent Member State.

In the PKI-based model used in the pilots, this verification is performed by checking revocation and status information published by the issuing authority, such as certificate revocation lists (CRLs), status lists, or equivalent machine-readable status services defined at the Union level. These

mechanisms allow the verifier to determine whether the credential has been revoked, suspended, or remains active, without requiring direct, case-by-case contact with the issuing institution.

The Austrian hospital's system performs these checks automatically as part of the verification flow, using trusted metadata and endpoints published by Spain. The result confirms that Maria's EHIC is still valid for coordination purposes at the time of treatment.

Privacy and Reliability Characteristics

This approach avoids creating unnecessary privacy risks. Verification does not require the Austrian hospital to notify Spanish authorities that Maria is receiving treatment at a specific location or time. The issuing institution publishes status information once, and verifiers consult it independently. This prevents the accumulation of detailed usage logs at the issuing authority that could otherwise reveal travel patterns or health-related behaviour.

From an operational perspective, PKI-based status checking also improves reliability in emergency scenarios. Verification does not depend on real-time human interaction with Spanish authorities or on office opening hours. Status information can be made highly available through redundant infrastructure, ensuring that verification remains possible even if core administrative systems are temporarily unavailable.

Layer 3: Secure Presentation and Exchange (OpenID-Based Interaction)

Communication Flow and User Experience

The actual interaction between Maria's EUDI Wallet and the Austrian hospital's registration system is handled through standardised presentation protocols, such as OpenID Connect for Verifiable Presentations (OIDC4VP). When the hospital initiates verification - typically by displaying a QR code or enabling an NFC-based interaction—this triggers a structured request that Maria's wallet can process regardless of the wallet provider or Member State of issuance.

Maria's wallet prepares a presentation that may combine multiple attestations, such as base identity data and the EHIC credential, and applies selective disclosure so that only the information necessary for coordination and billing is shared. The hospital's system verifies the cryptographic seals, checks current validity through PKI status mechanisms, and obtains sufficient assurance to proceed with treatment and administrative processing without delay.

Summary

This PKI-based architecture demonstrates that pluralistic trust coexistence does not require a single trust technology. In the social security domain, long-established PKI infrastructures - augmented by standardised metadata, status information, and modern presentation protocols - can support legally significant, time-critical cross-border scenarios. The result is an operationally robust and legally sound transaction that functions under real-world conditions, where failure would have immediate consequences for patient care, institutional liability, and the effective operation of EU social security coordination.

Table 8: The Complete Transaction Timeline - Three Trust Layers Working Together[9]

Time	Action	Trust Layer	What Happens Technically
T+0 sec	The hospital registration system displays QR code	OpenID	Verification request encoded in QR, including hospital identity and requested attributes
T+2 sec	Maria scans the QR code with her EUDI Wallet	OpenID	Wallet decodes the request and identifies required credential types
T+3 sec	Wallet retrieves EHIC credential from secure storage	Local	Credential decrypted using keys bound to Maria's device
T+4 sec	Wallet displays consent request in Maria's language	OpenID + GDPR	Clear explanation of the requested data, purpose, and verifier
T+4 sec	Wallet shows data to be shared:✓ Confirmation of insurance coverage✓ Policy identifier for coordination and billing✓ Validity period✗ No home address✗ no medical history✗ no unrelated credentials	Selective Disclosure	Wallet filters attributes according to the request and policy
T+6 sec	Maria approves sharing using biometric authentication	User Consent	Biometric confirms user intent to proceed
T+7 sec	Wallet creates a verifiable presentation	PKI	Presentation cryptographically signed by the wallet
T+8 sec	Presentation transmitted to the hospital system	OpenID	Encrypted transmission using standardised protocol
T+9 sec	Hospital verifies wallet and presentation signature	PKI	Confirms the integrity and authenticity of the presentation
T+9 sec	Hospital extracts EHIC credential	OpenID	Standardised credential format enables automatic parsing
T+10 sec	Hospital verifies the issuer seal on EHIC	PKI	Seal validated against Spanish trust anchors
T+11 sec	Hospital checks credential status	PKI Status Lists	Status queried via published revocation/status endpoints
T+12 sec	Status confirmation returned: credential valid	PKI Status	Confirms EHIC has not been revoked or suspended
T+13 sec	Hospital system displays "Coverage verified"	All Layers	Confirmation available for administrative processing
T+13 sec	Administrative registration proceeds	Business Logic	Treatment proceeds with coordination assurance

[9] See Bauer, G., & Alamillo, I. (2025) and Bauer, G., Gabel, H., Hilmar, K., Ilsøe, L., & Kaaber, C. (2025)

Comparative with the Traditional Process

Step	Action	Time	Reliability
1	Patient presents physical EHIC card	0-2 min	The card may be forgotten, damaged or expired
2	Staff manually records card details	2-5 min	Data entry errors are common
3	Staff attempts phone verification with the issuing authorities	5-30+ min	Often not feasible due to language barriers, office hours, or different procedures
4	Card accepted without verification	Immediate	Fraud and reimbursement risk shifted downstream

The Transformation in Real Terms:

The digital process reduces verification time from minutes—or, in many cases, impractical phone-based attempts—to seconds, while providing objective assurance through cryptographic verification rather than discretionary trust. Reliability improves because the process does not depend on physical documents, manual transcription, or synchronous human interaction with foreign authorities. Each verification either succeeds with a clear confirmation or fails with an explicit technical reason (e.g. expired credential, revoked status, connectivity issue), allowing staff to respond appropriately rather than relying on assumptions.

What This Demonstration Shows

- ✓ **Technical feasibility:** Traditional PKI-based trust, status verification, and OpenID presentation operate coherently within a single transaction.
- ✓ **Institutional viability:** Existing social security PKI infrastructures integrate with modern wallet-based verification without requiring replacement.
- ✓ **User acceptability:** An ordinary citizen can complete the process independently under stress.
- ✓ **Legal compliance:** The workflow aligns simultaneously with eIDAS requirements for electronic attestations, GDPR principles, and social security coordination rules.
- ✓ **Scalability:** The architecture supports large transaction volumes using established trust and distribution mechanisms.
- ✓ **Privacy protection:** Selective disclosure and decoupled status checking reduce unnecessary data exposure.
- ✓ **Operational performance:** End-to-end verification completes within timeframes compatible with emergency healthcare settings.

The Bottom Line for Policy and Deployment:

This architecture is not a theoretical construct derived solely from specifications or laboratory simulations. It has been implemented, tested, and operated under real-world conditions involving actual institutions, authentic credentials with legal and financial consequences, and citizens whose health and welfare depend on systems functioning reliably under time pressure. The pilots provide empirical evidence that the core technical components perform as intended: the protocols interoperate across heterogeneous national systems, cryptographic verification delivers the expected level of assurance, privacy protections function in practice rather than merely in principle, and legally recognised electronic attestations are accepted across borders in accordance with eIDAS requirements.

These results substantially reduce uncertainty regarding technical feasibility. They demonstrate that secure, privacy-preserving, cross-border verification of social security coordination credentials

is operationally achievable using existing infrastructures and standards, even in time-critical healthcare scenarios and across diverse institutional environments.

What remains for successful deployment at European scale is therefore not additional proof-of-concept work to establish basic technical viability. The remaining challenges are systemic rather than technical. As documented in Section 5, they concern sustainable funding models, legal and interpretative fragmentation, governance and coordination gaps, verifier onboarding and interoperability at scale, and user experience risks in high-pressure operational settings. Addressing these challenges requires deliberate execution of the policy interventions set out in Section 6, structured around the five proposed action pillars.

The technology has reached a level of maturity sufficient for production use. The decisive question is no longer whether the architecture can work, but whether the necessary political, institutional, and organisational conditions will be put in place to enable it to operate effectively at the European scale.

5 Systematic Barriers & Challenges

DC4EU solved a complex technical problem: engineering a hybrid architecture integrating EBSI, OpenID Federation, and PKI/eIDAS into a functioning system capable of issuing and verifying credentials across borders. More than two years of piloting demonstrated conclusively that the technology works, protocols function reliably, and security properties hold under real-world conditions. This technical success, however, exposed five foundational barriers at the EU level that now block the transition from pilot success to production deployment at scale.

These barriers are systematic rather than isolated, affecting the entire ecosystem rather than particular institutions or sectors. They emerged consistently across both Education and Social Security pilots despite significant differences between those domains, suggesting they reflect structural issues in European digital infrastructure deployment rather than sector-specific challenges. Each barrier emerged from observing where institutional progress stalled despite technical capability: universities uncertain about sustaining operations after project funding expires, verifiers refusing technically compliant credentials issued through unfamiliar mechanisms, sectors implementing incompatible metadata standards without coordinating authority, integration costs forcing smaller institutions to abandon participation, and citizens requiring manual intervention for transactions that should be automated.

These five barriers - unsustainable funding, legal fragmentation, technical interoperability gaps, governance fragmentation, and user experience failures - form an interconnected system. Addressing only some while ignoring others will not enable successful deployment. Sustainable funding without legal clarity leaves institutions uncertain whether investments will prove useful. Legal harmonisation without governance coordination creates fragmented interpretations. Governance structures without funding cannot enforce decisions. Technical interoperability without user-first design creates systems that work in theory but fail in practice. The barriers must be addressed comprehensively through coordinated action across the five pillars that Section 6 proposes.

5.1 Legal Foundations & Regulatory Fragmentation

The revised eIDAS Regulation provides comprehensive legal certainty at the regulatory level, establishing clear requirements for credential types, trust service providers, and cross-border recognition obligations. Yet this robust EU-level framework has not prevented regulatory fragmentation threatening to undermine automatic cross-border recognition. The problem manifests in how Member States interpret the relationship between technical trust mechanisms and legal recognition obligations, creating situations where credentials meeting all legal requirements face rejection based on technical implementation details that should be irrelevant.

The Core Problem: Credential Discrimination

Social Security pilots demonstrated that EHIC and PDA1 credentials can be issued and verified reliably using established national PKI infrastructures, standardised metadata, and revocation or status mechanisms in a manner consistent with the eIDAS framework and the EU social security coordination regulations. Implemented as Public Body Electronic Attestations of Attributes, these credentials achieved high technical assurance in practice and supported secure cross-border verification within the EUDI Wallet ecosystem.

At the same time, pilot experience exposed a critical deployment risk directly addressed by the policy recommendations in Section 6. Verifiers in some Member States hesitated to rely on credentials issued through unfamiliar technical or governance paths, not because of deficiencies in security or integrity, but due to uncertainty regarding legal recognition, acceptance obligations, and potential liability exposure. In particular, verifiers questioned whether reliance on a Public Body EAA issued by a foreign public authority carries different legal or financial risk than reliance

on credentials issued under more familiar trust arrangements, even where the applicable technical and regulatory requirements are met. This uncertainty reflects gaps in common interpretative guidance and coordinated governance, underscoring the need for early legal clarification, harmonised governance mechanisms, and verifier-focused operational support as preconditions for large-scale deployment.

How Fragmentation Undermines Regulation

If Member States develop divergent interpretations of which credentials must be accepted and under what conditions, cross-border recognition risks becoming contingent on bilateral practices rather than on the uniform application of Union law. In such a scenario, a credential that is routinely accepted in one Member State may be questioned or rejected in another, not because of differences in cryptographic security or issuance quality, but because national authorities have formed different views on acceptance obligations, liability exposure, or supervisory responsibility. Pilot experience indicates that once such interpretations are embedded in operational systems and verifier workflows, they are difficult and costly to reverse.

The legal framework seeks to prevent this outcome by enabling recognition across different issuance models when credentials comply with the applicable eIDAS and sectoral requirements and achieve the required level of assurance for their intended use. However, eIDAS does not establish automatic legal equivalence between all categories of Electronic Attestations of Attributes. Public Body EAAs and Qualified EAAs remain distinct legal instruments with different supervisory regimes and legal effects, even where their technical assurance characteristics may be comparable. The challenge identified in practice is therefore not a lack of legal basis for cross-border use, but insufficiently clear, authoritative guidance on how verifiers should assess acceptance obligations and liability when confronted with compliant but unfamiliar credential types. Addressing this gap is central to the Legal Clarity and Governance pillars: without common interpretative guidance and coordinated enforcement, regulatory intent risks being undermined by fragmented implementation.

Table 9: Legal Fragmentation Manifestations

Fragmentation Type	How it Manifests	Impact on Deployment	Policy Gap
Technical Source Discrimination	Verifiers reject PuB-EAAs from authentic sources, demanding QEAAs despite equivalent assurance	Creates a false credential hierarchy; disadvantages public sector issuers	No authoritative EC guidance on equivalence
Liability Uncertainty	Verifiers are unsure whether accepting foreign credentials creates greater liability	Defaults to rejection as "safer" option; undermines recognition	No standardised verifier liability framework
Divergent Interpretations	Member States develop different views on recognition obligations	Same credential accepted in some countries, rejected in others	No common interpretative guidance from EC
Informal Trust Hierarchies	Verifiers accept familiar sources more readily than equivalent unfamiliar sources	Creates bilateral recognition instead of multilateral system	No enforcement mechanism for non-discrimination

The Urgency of Authoritative Guidance

The Commission must publish authoritative common interpretative guidance establishing authoritative interpretative guidance on recognition and acceptance obligations across different compliant trust architectures - The guidance must state unambiguously that verifiers cannot lawfully reject high-assurance credentials based solely on technical issuance mechanism when credentials meet equivalent assurance standards. A credential that complies with the applicable

eIDAS and sectoral requirements must not be rejected solely based on the technical trust architecture used for its issuance..

The guidance must address verifier liability explicitly. Institutions currently operate without understanding whether accepting foreign credentials issued through unfamiliar mechanisms creates greater liability than rejecting legally valid credentials. This uncertainty drives risk-averse behaviour. The guidance should establish that verifiers acting in good faith and following standard verification procedures-checking signatures, confirming non-revocation, validating issuer authority-bear no greater liability for accepting compliant foreign credentials than for accepting equivalent domestic credentials.

Without clarity established quickly, divergent national interpretations will become embedded in operational systems, procedures, and institutional cultures. Legal interpretations developed during initial deployment tend to persist through path dependency even after being recognized as problematic, because changing them requires modifying regulations, updating procedures, retraining staff, and potentially rebuilding systems designed around initial interpretations.

5.2 Technical & Interoperability and ARF gaps

Successful coexistence of multiple trust models requires more than protocol compatibility: it demands a mandated governance and semantic layer bridging conceptual and operational gaps between modern blockchain-based registries and legacy PKI systems, between federated identity models and centralised authentication, between different national approaches to metadata and schemas. This bridging infrastructure does not currently exist in funded, operational form, and its absence prevents institutions from achieving cost-effective integration at the deployment scale.

The Harmonisation Gap

OpenID Federation successfully solved immediate interoperability challenges for real-time verification, demonstrating through eduGAIN integration how the EUDI Wallet works with established federated identity systems. However, a significant gap remains in aligning governance structures and semantic models of credentials issued through EBSI Verifiable Data Registries versus those issued through national PKI and eIDAS trust chains predating blockchain technologies by decades.

Consider institutions attempting to verify credentials arriving through either technical path without advance knowledge of which path a credential uses. EBSI-issued credentials contain governance metadata describing EBSI-specific accreditation chains, trust framework references, and policy identifiers. PKI-issued credentials reference certificate chains conforming to eIDAS conventions, QTSPs on national trusted lists, and trust anchors published through decades-old PKI mechanisms. Both approaches are valid and legally compliant, expressing equivalent trust relationships through fundamentally different technical and semantic models.

Without a common semantic layer translating between models, institutions must maintain parallel verification logic for each approach, effectively doubling integration complexity. A verification system must understand both EBSI governance metadata and PKI certificate chains, both EBSI policy references and eIDAS trust list entries, both EBSI revocation registries and PKI certificate revocation mechanisms. This duplicated logic increases development costs, creates more error opportunities, complicates testing, and makes ongoing maintenance more expensive as both models evolve independently.

The Integration Cost Barrier

The Architecture Reference Framework provides technical specifications for interoperability - data formats, protocol sequences, security requirements - with appropriate rigour. What the ARF does

not solve is semantic alignment when different governance models use different conceptual frameworks to express equivalent information. The ARF can specify that credentials must use particular formats and support specific protocols, but it cannot mandate how institutions map between different governance models or resolve semantic differences in how credentials describe functionally equivalent attributes.

This gap must be addressed through a European Harmonisation Layer – that is, funded infrastructure providing common metadata standards, schema translation services mapping between credential formats, governance mapping rules explaining how trust relationships in one model correspond to trust relationships in another, and verification protocols working consistently regardless of which trust model issued the credential. The Harmonisation Layer is not merely technical documentation or recommended practices institutions might adopt: it must be funded development producing operational services, reference implementations institutions can deploy, and testing infrastructure validating correct operation.

Member States also urgently require dedicated technical tooling and reference architectures for integrating legacy national IT systems - particularly PKI backends of Social Security and similar sectors operating decades-old systems - with the EUDI Wallet ecosystem's modern protocols and data models. Integration costs documented during DC4EU piloting ranged from €250,000 to €500,000 per institution for organizations without standardised tooling or reusable components. These costs reflect substantial engineering work bridging systems never designed to interoperate: connecting to legacy databases using outdated query languages, mapping between credential formats designed decades apart, managing credential lifecycle events in systems built before digital credentials existed, and providing verification interfaces that existing business logic can consume.

Table 10: Technical and Interoperability Barriers

Barrier	Manifestation	Impact	Required Solution
Semantic Misalignment	EBSI and PKI credentials use different metadata, governance references, and trust anchors	Verifiers must build dual systems; high complexity and cost	European Harmonisation Layer providing schema translation and governance mapping
Legacy System Integration	Social security PKI backends cannot directly interface with EUDI Wallet protocols	€250K-500K per institution in custom integration work; prohibitive for small agencies	Reference implementations, integration proxies, and toolkits are reducing integration work by 70-80%
Missing Coordination	Each institution solves the same integration problems independently	Duplicated effort across hundreds of institutions; inconsistent solutions	Funded development of common integration patterns and reusable components
Evolving Standards	ARF specifications change as implementation experience accumulates	Early implementations become outdated; retrofitting expensive	Versioning strategy and migration tooling enabling smooth transitions

Standardised tooling could reduce integration costs by seventy to eighty percent for typical scenarios by providing reusable components: database connectors for standard legacy database systems, credential format converters implementing standard mappings, lifecycle event managers handling issuance and revocation workflows, and verification interfaces providing standard APIs that multiple business applications can consume. Making this tooling available as open-source

software with comprehensive documentation would dramatically lower barriers for institutions viewing EUDI Wallet integration as beyond their technical and financial capabilities.

The cost reduction matters not merely for saving money but for determining whether comprehensive coverage is feasible. If only the largest and best-funded institutions can afford integration, deployment will be limited to a fraction of credential issuers and verifiers necessary for genuine citizen value. A citizen whose local municipality cannot afford integration gains no benefit from their national capital's perfect systems. The system's value depends on comprehensive coverage enabling credentials to be used everywhere citizens need them.

5.3 Governance & Operational Fragmentation

The challenge extends beyond technical compliance with the Architecture Reference Framework to encompass institutional readiness and cultural transformation required across diverse public sector organizations. The ARF provides comprehensive technical specifications, protocols systems must implement, data formats they must support, security properties they must maintain. What technical specifications alone cannot accomplish is mandating institutional readiness or driving cultural shifts required for successful implementation across organizations with fundamentally different understandings of their missions, priorities, and relationships with citizens.

The Institutional Transformation Challenge

Public sector bodies in education, social security, healthcare, and professional licensing must transform not merely technical systems but operational processes, organizational structures, staff competencies, and institutional cultures. A university must shift from viewing diplomas as paper documents it issues once and archives permanently to seeing them as digital credentials issued into citizen-controlled wallets where the institution no longer maintains direct oversight. This represents fundamental change in the institution's relationship with graduates and conception of what credential issuance means.

A social security agency must evolve from managing physical card distribution through postal services to maintaining digital credential registries with real-time status updates, supporting instant issuance into wallets, and handling revocation scenarios that may never occur with physical cards. These changes affect organisational structure by requiring new staff roles, budget allocation by shifting resources from card production to digital infrastructure, staff competencies by requiring training on unfamiliar technologies, and institutional identity by changing how the organization conceives of its core functions.

The pilot revealed that forty percent of participating organizations reported receiving inadequate guidance from national governments about what they are responsible for implementing, by when, with what resources, and to what standards. This absence of clear direction leaves institutions attempting to interpret EU regulations and technical specifications without national-level context needed for informed decisions about priorities, resource allocation, and implementation approaches aligning with national strategies.

The Sectoral Silo Problem

Fragmentation extends beyond individual institutions to affect sectoral governance structures operating with substantial autonomy. Education ministries and social security agencies often report through different governmental chains, follow distinct regulatory frameworks that may not be well coordinated, and pursue separate strategic priorities reflecting their different missions. When these sectors attempt EUDI Wallet integration, they may adopt incompatible metadata standards based on different interpretations, divergent approaches to credential schemas reflecting different assumptions, or conflicting approaches to privacy and consent management based on different legal advice.

Without a coordinating authority capable of imposing alignment when necessary, each sector optimizes its own implementation in ways creating barriers to cross-sectoral credential use. A student might find educational credentials work seamlessly within education for university admissions but cannot be easily used when applying for social security benefits depending on proving enrolment status. A worker might find professional qualification credentials issued by licensing authorities do not interoperate with employment verification systems because credential schemas were designed independently.

Table 11: Governance Fragmentation Dimensions

Fragmentation Level	How it Manifests	Consequence	Current Gap
Institutional	40% of institutions reported unclear roles and responsibilities	Inconsistent decisions; parallel efforts waste resources	No clear national guidance on implementation responsibilities
Sectoral	Education and social security develop incompatible metadata standards	Credentials work within sectors but not across them	No cross-sectoral coordination authority
National	Member States pursue independent approaches without coordination	27 different national implementations; interoperability at risk	No top-level governance body with enforcement authority
Temporal	Early implementations become incompatible with later standards	Retrofitting costs 3-5x more than coordinated deployment	No coordination mechanism prevents premature divergence

The Coordination Vacuum

The risk of siloed operations emerged repeatedly during DC4EU piloting. Education and social security work packages initially developed different approaches to similar technical challenges because they operated independently with limited cross-sectoral coordination. The project team eventually established coordination through regular meetings, shared technical working groups, and deliberate alignment efforts. But this required substantial effort and conscious attention that would not occur spontaneously in production environments without clear governance mandates and dedicated coordination resources.

The lesson generalises: sectoral autonomy, while valuable for enabling domains to address specific needs, becomes a liability when implementing infrastructure that must function coherently across all sectors. Educational credentials gain maximum value when usable not only for academic purposes but also for employment verification, professional licensing, and social security eligibility. Realising this value requires coordination ensuring credentials issued in one sector can be understood and verified in others without requiring citizens to obtain multiple credentials attesting to the same underlying facts.

The solution requires establishing a top-level governance body with genuine political authority extending beyond advisory functions. This body must have an explicit mandate to define and enforce common standards where commonality is necessary for interoperability, while respecting legitimate sectoral expertise and institutional autonomy for decisions not affecting cross-sectoral or cross-border functioning.

5.4 Funding & Resources

The technical blueprint for the EUDI Wallet is complete, thoroughly validated, and ready for production deployment. The primary failure mode at this point is operational atrophy resulting from inadequate and unpredictable financing treating permanent infrastructure as temporary research projects. Current project-based funding models are fundamentally unsuited for

supporting long-term operational tasks of maintaining pan-European trust infrastructure that must function reliably for decades while evolving continuously.

The Immediate Crisis: Pilot Funding Cliff

DC4EU operates under grant funding terminating in July 2025, creating an immediate crisis for institutions that invested substantial resources over three years building integration capabilities, developing expertise, training staff, and establishing operational procedures. When project funding ends, what happens to the technical infrastructure built through intensive piloting? What happens to trained personnel who developed a deep understanding through hands-on experience? What happens to institutional knowledge accumulated through solving hundreds of integration challenges? Without continuity funding bridging from project termination to sustainable operational support, the default outcome is institutional capacity loss as personnel move to more secure positions, systems shift to maintenance-only mode, and organizational focus shifts to other priorities with clearer resource commitments.

Survey data documents this risk: sixty percent of small public bodies stated they cannot sustain EUDI Wallet integration beyond twelve to eighteen months without guaranteed multi-annual funding. Thirty-five percent reported already losing key technical staff to private sector opportunities during the pilot phase because project-based employment created too much career uncertainty. These are not abstract future risks-they are documented losses already occurring.

The Structural Problem

Financial requirements for sustained operation extend beyond personnel costs. The complex pluralistic architecture requires ongoing investment in maintaining the European Harmonisation Layer, operating bridges between EBSI and PKI systems, updating schemas and standards as requirements evolve, providing technical support to implementing institutions, and managing governance processes keeping diverse systems aligned. These are permanent operational costs intrinsic to running European infrastructure, not one-time development expenses disappearing after initial deployment.

Attempting to fund permanent operational infrastructure through successive project grants creates multiple pathologies. It forces institutions to treat ongoing operations as research activities generating novel insights rather than routine maintenance. This distorts budgeting and planning, as institutions cannot make multi-year commitments when next year's funding remains uncertain. It creates personnel instability making retention nearly impossible. It requires constant proposal writing and justification for activities that should be accepted as necessary ongoing costs. Most fundamentally, it signals the Commission views the EUDI Wallet as experimental rather than essential infrastructure, undermining the institutional commitment needed for serious implementation.

Table 12: Funding Model Comparison

Dimension	Current: Project Grants	Required: Production Funds	Impact of Current Model
Duration	2-4 years per grant	Multi-annual (5+ years)	Constant reapplication overhead; planning uncertainty
Predictability	Uncertain until approved	Guaranteed within the budget cycle	Cannot commit to long-term initiatives or personnel
Personnel	Project-based contracts	Permanent positions	35% already lost key staff; retention impossible
Justification	Must argue for "innovation"	Accepted operational cost	Forces artificial framing of routine maintenance

Focus	Deliverables and milestones	Reliable service operation	Optimises for visible outputs over operational excellence
Small Institution Access	Limited (lack of grant-writing capacity)	Allocated by need	60% cannot sustain beyond 12-18 months
Administrative Burden	High (proposals, reporting)	Appropriate for operations	Substantial staff time is diverted from actual work

The Required Solution

The Commission must establish multi-annual, non-project-based Production Funds supporting both operational management of core European infrastructure and the institutional capacity building Member States require. Funding must provide predictability across five-year minimum horizons so institutions can make rational staffing decisions, plan capability improvements, and commit to long-term initiatives. Administrative requirements should be appropriate for operational funding rather than imposing research-project-style reporting on routine infrastructure maintenance.

Individual institutions require €50,000 to €150,000 annual operational funding depending on scope and complexity. Core European infrastructure requires dedicated funding for permanent staff, system operation, security monitoring, and ongoing development. Across the ecosystem, annual operational costs will be measured in hundreds of millions of euros - substantial but not unprecedented for critical European infrastructure serving 450 million citizens.

These costs should be evaluated against the economic value created: a ninety-five percent reduction in administrative costs for credential verification, enabling previously impractical cross-border mobility, preventing fraud through real-time verification, and eliminating weeks of delay. The Commission should commission a comprehensive economic impact analysis quantifying these benefits. The analysis will almost certainly show substantial net positive returns, but decision-makers need explicit documentation.

Institutions face immediate decisions as DC4EU funding has expired. Capacity losses cannot be recovered quickly enough to meet the 2026 mandate. Personnel who leave will not easily return. Institutional knowledge that dissipates must be painfully rebuilt. Systems entering maintenance-only mode take time to reactivate. Continuity depends on avoiding a funding gap forcing institutions to abandon work in progress.

5.5 User Experience & Trust

The most significant threat to long-term citizen adoption and trust is the "data courier" risk when institutions fail to automate secure data exchange, forcing citizens to manually transport information between systems that should communicate directly. This experience directly contradicts the EUDI Wallet's value proposition of seamless digital services and will drive rapid abandonment if it characterises actual deployment.

The Data Courier Scenario

The scenario unfolds when institutional integration remains incomplete. A citizen presents a digital credential from their EUDI Wallet to a service provider whose systems cannot automatically verify the credential. Rather than acknowledging their technical limitation, the provider asks the citizen to "also provide a paper copy" or "have the issuing institution send verification through official channels." From the provider's perspective, this seems reasonable. From the citizen's perspective, the digital wallet just created additional work: they still need the paper version they thought they could discard.

This destroys the value proposition immediately. Why carry a digital credential if you also need the paper version? The wallet becomes additional burden rather than a solution. Citizens generalise

from one bad experience to broader scepticism. If the wallet failed once, it might fail again, so they continue carrying paper documents "just in case."

The Measured Failure Rate

User testing during DC4EU revealed that twenty-five percent of pilot transactions required manual intervention due to verification system incompatibilities, credential format issues, or missing metadata. This might seem acceptable during pilots where technical difficulty is expected. But it would be catastrophic in production where citizens expect systems to simply work. One in four transactions failing is one in four reasons to abandon the system.

Post-pilot surveys showed user satisfaction dropped forty percent when data courier scenarios occurred: citizens perceived the technology as broken. More tellingly, seventy percent stated they would revert to paper documents if digital verification "didn't just work" reliably. This represents stated intention from people who experienced both working and failing scenarios.

Table 13: User Experience Failure Patterns

Failure Pattern	How it Occurs	Citizen Experience	Long-Term Consequence
Data Courier	Verifier cannot process the digital credential; requests paper backup	"Digital wallet is extra work, not a solution"	Citizens maintain paper documents; the wallet becomes unused
Manual Intervention	System error requires staff assistance	"This is too complicated; paper is easier"	Citizens avoid digital credentials for important transactions
Inconsistent Acceptance	Credential works in some places, rejected in others	"I can't rely on this; it might not work when needed"	Citizens lose trust; share negative experiences
Unexplained Errors	The system fails with technical errors citizen cannot fix	System fails with technical errors citizen cannot fix	Citizens abandon wallet; view technology as unreliable

Root Causes and Required Solution

Underlying causes are predictable: institutions implement credential issuance because it is visible and creates positive publicity but fail to update verification systems because that work is less visible and more complex. Verifiers build capability for one trust model but not others, creating arbitrary acceptance patterns. Legacy systems lack interfaces to consume digital credentials directly, forcing manual transcription.

The solution requires enforcing user-first design principles through policy requirements rather than encouraging better practices. All future deployment funding must be conditional on demonstrating elimination of data courier scenarios through genuine automated data exchange. Wallet providers and issuing bodies must implement automated, secure data flows. Verifiers must handle all conformant trust models, not just familiar approaches. Representative users completing typical tasks should achieve seventy-five percent success rate without manual intervention, assistance, or fallback to paper documentation.

Systems failing this threshold should not be considered compliant regardless of technical adherence to specifications. This user-centric compliance standard focuses implementation effort on delivering genuine value rather than checking technical boxes while leaving users to navigate dysfunctional processes. When digital tools create more friction than paper processes they replace, citizens will abandon them regardless of technical sophistication. Rebuilding trust after failed deployment is exponentially harder than building it correctly from the start.

6 Recommendation: From Technical Blueprint to Political Execution

The pluralistic architecture validated by DC4EU provides the definitive blueprint for EUDI Wallet deployment. Technical questions have been answered through two years of intensive piloting. Success now hinges on political will and operational execution at an unprecedented scale.

The Timeline Reality

Member States face a legal mandate to deploy functional wallets by the end of2026. That leaves less than twelve months.

The arithmetic is unforgiving:

- **6 months:** Governance establishment and funding allocation
- **4 months:** Technical deployment and integration
- **2 months:** Testing and citizen onboarding

There is no buffer for delay. The 2026 mandate is at severe risk without immediate action.

Strategic Framework: Five Core Action Pillars

The complex pluralistic architecture validated by DC4EU provides the definitive blueprint for the EUDI Wallet. The system's success now hinges not on technology, but on political will and operational execution. To overcome the systemic barriers identified in Section 5 and ensure full deployment by the 2026 mandate, the European Commission must immediately transition to a production footing by funding and enforcing the following Five Core Action Pillars.

Table 14: Action Pillars Overview

Pillar	Primary Objective	Critical Deadline	Responsible Actors	Consequence of Delay
Legal Clarity	Eliminate credential discrimination; establish verifier liability	Q1 2026	EC Legal Services, Member States	Legal silos crystallise; cross-border recognition fails
Harmonised Governance	Prevent fragmented national approaches	Q1 2026	EC, Member States, Sectoral Authorities	27 incompatible implementations; mandate fails
Sustainable Funding	Secure operational funding immediately	Q1 2026	EC (DG BUDG, DG Digital), Member States	Institutional capacity already lost; further atrophy is inevitable
Architectural Interoperability	Reduce integration costs by 70-80%	Mid-2026	Technical WGs, Member States	Integration is prohibitively expensive; coverage is not feasible
Citizen Trust	Achieve 75% task completion without intervention	Mid-2026	Wallet Providers, Issuers, Verifiers	Poor experience drives abandonment; trust erosion is permanent

6.1 Legal Clarity and Policy Harmonisation

Action Pillar Objective:

Eliminate legal silos and incentivise private sector uptake by establishing that credentials meeting equivalent assurance standards receive equivalent legal recognition, supported by clear operational specifications in the EU attribute catalogues.

The Critical Legal Distinction

Legal precision is paramount for policy implementation. Three credential types must be distinguished and harmonised within the **Implementing Regulation (EU) 2025/1569** framework:

- **Qualified Electronic Attestations of Attributes (QEAAs)**: Issued by QTSPs subject to strict oversight, listed on EU Trusted Lists
- **Public Body Electronic Attestations of Attributes (PuB-EAAs)**: Issued by authentic sources within public sector organizations
- **Non-Qualified Electronic Attestations of Attributes**: Issued by accredited institutions meeting high assurance standards

The Equivalence Mandate

A credential that complies with the applicable eIDAS and sectoral requirements must not be rejected solely based on the technical trust architecture used for its issuance. Current practice reveals "credential discrimination", verifiers often refuse PuB-EAAs from universities, demanding QEAAs despite equivalent assurance levels.

Current practice reveals credential discrimination. Verifiers refuse PuB-EAAs from universities, demanding QEAAs from QTSPs despite equivalent assurance. This contradicts the fundamental goal of enabling seamless cross-border use based on actual assurance levels.

Required Actions

1. Operationalise the Schema and Attribute catalogues (By March 2026)

- The European Commission must prioritise the completion of the catalogues defined in IR 2025/1569. These are the essential tools for private and public sector onboarding.
- Populate Data Models: Fill the currently empty catalogues with the necessary interoperability and governance specifications.
- Technical Trust Specs: Include clear trust model specifications (EBSI, PKI/eIDAS, OpenID Federation) within the catalogues to allow entities to build awareness and begin technical integration.

2. Publish Common Interpretative Guidance (By March 2026)

The European Commission must publish authoritative guidance establishing:

- Legal equivalence across trust models (EBSI, PKI/eIDAS, OpenID Federation)
- Non-discrimination requirement: verifiers cannot reject credentials based on the technical issuance mechanism when assurance levels are equivalent
- Assurance-based acceptance: decisions must be based on verified assurance properties, not familiarity with specific approaches

The guidance must be formal Commission communication with legal weight, not technical recommendations.

3. Establish Standardised Verifier Liability Framework (By March 2026)

The framework must establish:

- Good faith protection for verifiers following standard verification procedures
- Primary obligations for national verifiers and public bodies to implement EU regulations
- Private sector clarity about obligations and protections
- Enforcement mechanisms with formal inquiry processes and corrective actions

Table 15: Legal Clarity Implementation Timeline

Milestone	Deliverable	Owner	Deadline	Status Trigger
Phase 1	**IR 2025/1569 Task Force/Working group established to fill Attribute Catalogue**	EC DG CONNECT, Member States	February 2026	Task Force operational
Phase 2	Legal Harmonisation Task Force established	EC Legal Services, Member States	February 2026	Task Force operational
Phase 3	Common interpretative guidance published	Task Force, EC	March 2026	Official publication
Phase 4	Verifier liability framework published	Task Force, EC	March 2026	Formal guidance available
Phase 5	Enforcement mechanism operational	Member States, EC	June 2026	Reporting process accessible

6.2 Harmonised Governance

Action Pillar Objective:

Prevent ecosystem fragmentation by transforming the European Digital Identity Cooperation Group (EDICG) into a top-level authority with the political and operational mandate to enforce common standards.

To ensure a successful 2026 rollout, the Commission and Member States must formally **strengthen and expand** the EDICG, established under Article 46e of Regulation (EU) 2024/1183 to move beyond purely advisory functions. The Group must be empowered to define and enforce standards where commonality is essential for cross-border interoperability.

The Governance Board Mandate

The Commission and Member States must formally establish a **Top-Level European Digital Identity Governance Board** with genuine political authority beyond advisory functions. The board must have explicit mandate to define and enforce standards where commonality is necessary for interoperability.

Core Responsibilities

- **Populate Attribute Catalogues:** Lead the definition of mandatory metadata standards, semantic models, and credential schemas within the **IR 2025/1569 catalogues**.

- **Resolve Sectoral Conflicts:** Act as the final arbiter when incompatible approaches emerge between domains (e.g., Education vs. Social Security).
- **Direct ARF Evolution:** Maintain the Architecture Reference Framework (ARF) as a "living document" updated by real-world operational experience.
- **Private Sector Liaison:** Establish formal mechanisms to incentivise and coordinate with private sector Relying Parties.
- **Compliance Monitoring:** Track implementation across Member States and trigger enforcement actions when alignment fails.

Governance Structure

- **Technical Expert Group: A permanent advisory body of technical experts to ensure specifications remain implementation-ready.**
- **Composition**: Member State representatives (voting), EC representatives (coordination), sectoral authority observers, technical expert advisors (non-voting)
- **Decision-Making**: Qualified majority voting (prevents single Member State blocking); unanimity only for sovereignty or legislative changes
- **Operational Model**: Quarterly strategic meetings, monthly working groups, permanent funded secretariat, published decisions

Table 16: Governance Board Functions

Function	Special Responsibilities	Authority Level
Standardisation	Define mandatory metadata standards and schemas within the **IR 2025/1569 catalogues**.	Mandatory for public bodies
Conflict Resolution	Resolve incompatible sectoral approaches	Binding on sectors
ARF Evolution	Update specifications based on operational experience	Mandatory for new implementations
Cross-Sectoral Coordination	Enable credentials to work across sector boundaries	Sets interoperability requirements
Compliance Monitoring	Track implementation, identify problems early	Can trigger enforcement
Enforcement Escalation	When voluntary compliance fails, escalate politically	Political authority backing

Establishment Timeline

- **February 2026**: Formal decision to reposition the EDICG with expanded operational terms of reference.
- **February 2026**: Membership designated, terms of reference finalised, secretariat funded
- **March 2026**: First meeting under the new mandate; priority given to filling the IR 2025/1569 catalogues.
- **April-June 2026**: Working groups develop common standards for immediate deployment

The board must be operational by April 2026 because coordination becomes exponentially more difficult after Member States commit to divergent paths.

6.3 Sustainable Funding and Institutional Capacity

Action Pillar Objective: Transition from short-term, project-based grant cycles to multi-annual operational funding preventing institutional capacity loss.

The Production Fund Model

The European Commission (DG BUDG- Directorate-General for Budget and DG Digital-Directorate-General for Digital Services, formerly DG Informatics) must establish a multi-annual, non-project-based funding mechanism (a "Production Fund") to support the operational management of core European infrastructure and institutional capacity building across all Member States.

1. Core European Infrastructure (Annual budget: €50-100M)

- European Harmonisation Layer operation
- EBSI infrastructure supporting government registries
- Technical support services
- Security monitoring and incident response
- Ongoing development addressing emerging requirements

2. Institutional Capacity Building (Annual budget: €200-400M across Member States)

- National and local public body integration capabilities
- Dedicated staff positions
- System operation and maintenance
- Training and professional development
- Technical infrastructure costs

Funding Characteristics

Production Funds differ fundamentally from project grants through five-year minimum funding cycles, predictable allocation based on objective criteria, operational focus with appropriate administrative requirements, needs-based distribution supporting small institutions, and explicit support for permanent staff positions.

Table 17: Funding Model Transformation

Aspect	Current: Project Funds	Required: Production Funds
Duration	2-4 years, uncertain renewal	5-7 years, guaranteed
Allocation	Competitive proposals	Formula-based on criteria
Justification	Innovation and deliverables	Operational necessity
Personnel	Project contracts	Permanent positions
Reporting	Detailed project management	Operational performance
Admin Burden	High (30-40% effort)	Low (5-10% effort)
Small Institution	Difficult access	Guaranteed allocation

Implementation Pathway

- **Q1 2026**: Commission proposes Production Fund; Member States agree to multi-annual commitment; budget authority established for 2026-2031 cycle

- **Q2 2026**: Allocation formula applied; funding agreements signed; payment schedules established
- **Q3 2026 Onward**: Production Fund fully operational

Economic Justification

Annual investment required: €250-500M across the EU. Documented benefits from pilots include a ninety-five percent reduction in verification costs, ninety-nine percent reduction in credential acquisition time, fraud prevention worth €100M+ annually, and enabling cross-border mobility worth billions. Conservative estimates suggest a 3:1 benefit-cost ratio within five years, increasing to 5:1+ as adoption scales.

Critical timing: Funding mechanisms must become operational by March 2026. DC4EU funding ended July 2025, creating a capacity loss gap that has already begun. Immediate action is required to prevent further atrophy.

6.4 Architectural Interoperability

Action Pillar Objective: Deploy European Harmonisation Layer and integration tooling reducing integration costs by seventy to eighty percent.

The European Harmonisation Layer

The Commission must mandate and fund the immediate deployment of comprehensive infrastructure bridging different trust models:

Core Components:

- **Schema Translation Services**: Map between EBSI and PKI credential formats; translate governance metadata
- **Governance Mapping Registry**: Document how trust relationships in different models correspond; publish in machine-readable format
- **Common Metadata Standards**: Define mandatory metadata all credentials must include; establish credential schemas for common use cases
- **Verification Protocol Abstraction**: Provide a unified verification API accepting credentials from any conformant trust model

Integration Tooling:

- **Reference Implementations**: Complete issuer, wallet, and verifier components as open source software
- **Integration Proxies**: Translation layers between legacy databases and EUDI Wallet protocols
- **Developer Toolkits**: Libraries for common programming languages handling cryptographic operations and protocol implementation
- **Testing Infrastructure**: Conformance, interoperability, load, and security testing

Table 18: Integration Cost Reduction

Integration Task	Cost Without Tooling	Cost With Tooling	Reduction
Legacy Database Connection	€50K-100K	€5K-15K	85-90%
Credential Format Mapping	€40K-80K	€5K-10K	87-88%

Verification Logic	€60K-120K	€10K-20K	83-85%
Security Implementation	€30K-60K	€5K-10K	83-85%
Testing and Validation	€40K-80K	€5K-15K	81-88%
Total Per Institution	**€220K-440K**	**€30K-70K**	**77-86%**

Deployment Strategy

- **Q1-Q2 2026**: Technical working groups design architecture; develop reference implementations; build integration proxies; deploy testing infrastructure
- **Q3 2026**: Selected institutions pilot deployment; tooling tested with real systems; documentation refined
- **Q4 2026**: Harmonisation Layer operational for all institutions; integration tooling available as open source; support services established

Critical Success Factors: Open source mandate for all components, comprehensive documentation beyond technical specs, and active community support with forums and dedicated help channels.

6.5 Citizen Trust and User Experience

Action Pillar Objective: Enforce user-first design eliminating data courier scenarios and achieving seventy-five percent independent task completion rate.

The Fundamental Principle

Citizens must never be forced to manually transport information between systems that should communicate directly. When verification fails, the failure should trigger a technical investigation, not demands that citizens obtain alternative documentation.

Mandatory User-First Design Requirements

All deployment funding must be conditional on demonstrating the elimination of data courier risks:

1. Automated Verification Workflows: Verifiers must implement automated verification handling all conformant credential types without manual intervention; integrate with business systems enabling immediate processing; handle errors by notifying administrators, not blaming users.

2. Selective Disclosure Implementation: All credential presentations must support selective disclosure with clear consent interfaces in plain language, granular control allowing approval or denial of specific attributes, visual indication of what is shared vs. private, and audit trails.

3. Error Communication and Recovery: When technical problems occur, systems must explain what went wrong in user-understandable language, provide actionable guidance, offer contact information for support, and give estimated resolution timelines.

Table 19: User Experience Requirements

Mandatory Capability	Requirement	Success Criteria
Automated Verification	Accept all conformant credential types; verify without manual intervention	95%+ verification attempts succeed automatically
Selective Disclosure	Share only requested attributes with explicit user approval	User approves 100% of sharing actions
Clear Communication	Explain sharing requests in plain language	80%+ users correctly understand requests

Error Recovery	System identifies and fixes problems without involving the user	Users receive a clear explanation and timeline
Cross-Platform Consistency	Same experience regardless of device or wallet provider	Users can switch without relearning

User Acceptance Testing as Compliance Gate

Systems must demonstrate user acceptance through rigorous testing with representative users, typical scenarios, realistic conditions, and independent evaluators. Success threshold: seventy-five percent of representative users successfully complete typical tasks independently without assistance, fallback to paper, or manual intervention. Systems failing to meet the threshold do not receive deployment approval.

Implementation Timeline

- **Q1-Q2 2026**: Develop user experience requirements and testing protocols; establish methodology and evaluation criteria; train independent evaluators
- **Q3-Q4 2026**: Mandatory user acceptance testing for all deployments; independent evaluators observe and score; results reported to governance board; failing systems receive remediation guidance
- **Ongoing 2027+**: Continuous monitoring of production systems; regular testing; user satisfaction surveys; feedback mechanisms

The Stakes

When digital tools create more friction than paper processes, citizens abandon them regardless of technical sophistication. The EUDI Wallet must be easier, faster, and more reliable than paper documents, or it will fail to achieve meaningful adoption. Europe cannot afford to treat user experience as secondary. User experience is the measure of whether the system actually works.

7 Metrics of Success: Key Performance Indicators for the 2026 Mandate

To ensure the EUDI Wallet meets its 2026 production mandate, clear accountability through verifiable benchmarks is essential. This section defines Key Performance Indicators (KPIs) measuring the execution and success of the Five Core Action Pillars detailed in Section 6. These metrics distinguish between quantitative impact targets demonstrating functional success and efficiency gains, and qualitative alignment milestones tracking completion of governance and legal frameworks.

Important Legal Caveat

Section 6's simplified convention using "QEAA" as umbrella terminology is suspended here. In these policy-critical performance indicators, legal distinctions between QEAAs (issued by Qualified Trust Service Providers), PuB-EAAs (issued by public body authentic sources), and Non-Qualified EAAs (issued by accredited institutions) are paramount. Pillar 6.1 specifically demands legal equivalence for all three types to ensure cross-border verification cannot be blocked on technical grounds when assurance levels are equivalent.

7.1 Quantitative Impact and Adoption Targets

These verifiable metrics demonstrate the functional success, efficiency gains, and mass adoption necessary to meet the 2026 mandate and validate the system's value proposition.

Table 20: Quantitative Performance Indicators

Metric	Target	Timeframe/Scope	Measurement Method	Baseline (DC4EU Pilots)
Verification Success Rate	95% successful cross-border credential verification (EHIC, PDA1, Educational Credentials)	24 hour transaction time	Automated monitoring of verification attempts across Member States	70% (first attempt, 12 Member States, no coordination)
Processing Time Reduction	60% reduction in processing time for cross-border student mobility and worker social security transfers	Post-rollout (measured over 18 months)	Comparison of average processing time: traditional vs. digital workflows	Traditional: 6-8 weeks; Digital: 45 seconds (pilot)
Administrative Cost Reduction	30% decrease in administrative costs for credential verification in the Education and Social Security sectors	Post-rollout (measured over 18 months)	Cost accounting comparing manual verification vs. automated digital verification	95% cost reduction documented in pilots
Member State Compliance	All 27 Member States issue functional EUDI Wallets	December 2026	Audit of Member State deployment status; functional testing	N/A (mandate deadline)
Cross-Sectoral Interoperability	80% of Member States achieve full cross-sectoral interoperability (credentials work across Education,	By December 2027	Testing of credential acceptance across sector boundaries	Limited sectoral silos in pilots

	Social Security, Healthcare)			
Citizen Adoption Rate	40% active adoption among mobile-enabled EU citizens using EUDI Wallets for education or social security services	Within three years of national rollout (by 2029)	Active wallet usage tracking; transaction volume analysis	N/A (pilot phase with limited users)
Verification Cost Per Transaction	€0 marginal cost per verification (after initial infrastructure investment)	Ongoing operational metric	Cost accounting of verification operations	Traditional: €250-500 per manual verification
Credential Issuance Time	< 24 hours from request to wallet delivery for standard credentials	Ongoing operational metric	Timestamp analysis of issuance workflows	Traditional: 7-14 days; Digital: 2-3 minutes (pilot)

Performance Indicator Notes:

Verification Success Rate (95% target): The seventy percent first-attempt success rate achieved during DC4EU pilots across twelve Member States with zero prior coordination provides the baseline. The ninety-five percent target for production deployment reflects expected improvements from implementing the five action pillars: legal clarity eliminating unjustified rejections, governance harmonisation reducing metadata incompatibilities, the Harmonisation Layer resolving semantic misalignments, and standardised tooling reducing implementation errors.

Processing Time Reduction (60% target): DC4EU demonstrated ninety-nine percent time reduction for specific transactions (credential verification: weeks to seconds). The more conservative sixty percent target for overall process improvement accounts for portions of cross-border procedures beyond credential verification that digital credentials cannot accelerate (e.g., substantive evaluation of qualifications, administrative decision-making).

Administrative Cost Reduction (30% target): While pilots showed ninety-five percent cost reduction for credential verification specifically, the thirty percent target for overall administrative costs recognises that credential verification represents only part of total administrative burden in Education and Social Security operations.

Citizen Adoption Rate (40% target): The forty percent adoption target within three years represents ambitious but achievable penetration given the mandatory nature of certain credentials (EHIC for travellers, PDA1 for cross-border workers) and the demonstrated user preference (seventy percent would abandon if systems "didn't just work," implying strong adoption if systems do work).

7.2 Qualitative Alignment with Policy Pillars

These milestones track completion and operational status of core governance and legal frameworks mandated by the policy pillars. Unlike quantitative targets measured through ongoing metrics, these represent discrete deliverables with specific completion criteria.

Table 21: Qualitative Alignment Milestones

Policy Pillar Alignment	Alignment Milestone	Milestone Target Status	Completion Deadline	Verification Method
Legal Clarity (6.1)	Legal Recognition Consistency achieved across all trust models (EBSI, PKI/eIDAS, OpenID Federation)	Uniform and enforceable guidance published; no legitimate credential rejections based on technical source	March 2026	Official Commission guidance published in the Official Journal or equivalent; enforcement mechanism operational
Legal Clarity (6.1)	Standardised Verifier Liability Frameworks established	Fully operational framework with clear good-faith protections	March 2026	Formal guidance document published; Member States acknowledge the framework
Legal Clarity (6.1)	GDPR and Privacy Compliance (Preventing Successful Litigation).	Zero successful legal challenges post-rollout.	Post-rollout (ongoing)	Legal case tracking; privacy impact assessments validated
Governance & Interoperability (6.2/6.4)	Trust Framework Maturity (EBSI, OpenID Federation, PKI interoperability)	Production-ready and stable infrastructure; all three trust models are operational	June 2026	Stability testing; uptime >99.5%; interoperability testing passed
Governance & Interoperability (6.2/6.4)	Formal Governance Procedures (Metadata, Standards, ARF evolution)	Documented and enforced through the Governance Board	April 2026	Governance Board operational; decisions published; compliance monitoring active
Sustainable Funding (6.3)	Institutional Readiness and Budgeting (Education/Social Security issuers)	Full operational capacity secured via self-sustaining long-term budget	March 2026	Production Funds operational; multi-annual budgets allocated; funding agreements signed
Architectural Interoperability (6.4)	European Harmonisation Layer deployed	Operational for all institutions; reduces integration costs by 70-80%	June 2026	Harmonisation Layer live; integration cost data validates reduction targets
Architectural Interoperability (6.4)	Reference implementations and integration tooling are available	Open source software published; comprehensive documentation; and community support is active	June 2026	GitHub repositories are public; download statistics; community forum and active
Citizen Trust (6.5)	User Experience Quality. (Core Task Completion Rate).	75% independent user success rate achieved in user acceptance testing	June 2026	Independent testing with representative users; results published
Citizen Trust (6.5)	Data Courier Scenarios eliminated	Zero mandatory manual data transport in standard workflows	June 2026	User journey audits; automated verification >95%

Milestone Notes:

Legal Recognition Consistency: This milestone is achieved when the Commission's common interpretative guidance is published with legal authority and enforcement mechanisms are operational. The metric of success is the absence of legitimate credential rejections based on technical source (EBSI vs. PKI vs. OpenID Federation) when credentials meet equivalent assurance

standards. "Legitimate" distinguishes from rejections based on genuine security concerns, expired credentials, or revoked status.

Verifier Liability Frameworks: Completion requires publication of formal guidance establishing good-faith protections for verifiers, clarifying primary obligations for national verifiers and public bodies, and providing private sector clarity. Member States must formally acknowledge the framework even if implementation requires national-level regulation.

GDPR Compliance Validation: While GDPR compliance is built into system architecture (as documented in Section 3.4), this milestone tracks the absence of successful legal challenges post-rollout. A successful challenge would indicate architectural or procedural gaps requiring remediation. Privacy impact assessments conducted by independent auditors provide proactive validation.

Trust Framework Maturity: Production-readiness is measured through stability testing (uptime exceeding 99.5% for critical infrastructure), interoperability testing (credentials from any trust model successfully verified by any compliant verifier), and load testing (systems handle expected transaction volumes without degradation).

Formal Governance Procedures: The Governance Board becomes operational when it holds its first meeting, publishes its first decisions, establishes compliance monitoring processes, and demonstrates enforcement capability (even if enforcement is not immediately necessary). Documentation must be publicly accessible enabling accountability.

Institutional Readiness and Budgeting: This milestone is achieved when Production Funds are operational, multi-annual budgets (five-plus years) are allocated to participating institutions, funding agreements are signed establishing clear terms, and payment schedules ensure institutions receive funding predictably. Survey data from participating institutions confirming budget security provides validation.

European Harmonisation Layer Deployment: Operational status requires that the layer is deployed in production environments (not merely development or testing), accessible to all institutions requiring integration support, demonstrably reducing integration costs (validated through before/after cost data from early implementers), and supported by active maintenance and support services.

Reference Implementations and Tooling: Availability is measured through public GitHub repositories containing complete, documented code, download statistics showing active adoption, comprehensive documentation including implementation guides and troubleshooting references, and active community forums where implementers can get support.

User Experience Quality: The seventy-five percent independent success rate is measured through formal user acceptance testing using representative users (not system designers or technical experts), typical credential presentation scenarios (not contrived simple cases), realistic conditions including time pressure and distractions, and independent evaluators not involved in system development. Testing protocols must be published enabling reproducibility.

Data Courier Scenario Elimination: This milestone is achieved when user journey audits confirm that standard workflows do not require citizens to manually transport information between systems, verification automation exceeds ninety-five percent (fewer than five percent of transactions require manual intervention), and error handling directs problems to system administrators rather than citizens.

7.3 Monitoring and Accountability Framework

Continuous Monitoring

The Governance Board established under Pillar 6.2 holds primary responsibility for monitoring these KPIs. Quarterly reports track progress against targets, identify emerging problems requiring intervention, highlight successful implementations worth replicating, and recommend corrective actions when targets are not being met.

Transparency and Public Reporting

All KPI data should be published publicly through a dedicated EUDI Wallet deployment dashboard accessible to citizens, media, and civil society. Transparency serves multiple purposes: enables democratic accountability for use of public funds, allows early identification of problems through external scrutiny, provides Member States with comparative data motivating performance improvement, and builds citizen confidence through demonstrated progress toward targets.

Accountability Mechanisms

When Member States or institutions fall significantly below targets, the governance framework must provide escalation mechanisms. Initial responses include technical assistance and resource support identifying root causes and providing remediation guidance. If voluntary improvement efforts fail, formal inquiries investigate why targets are not being met and what barriers exist. Finally, political escalation to Council level may be necessary for persistent non-compliance threatening overall mandate success.

Adaptive Refinement

These KPIs represent initial targets based on pilot experience and expert judgment. Operational experience during 2026 rollout will provide empirical data enabling refinement. The Governance Board should review targets annually, adjusting based on actual performance data, emerging technical capabilities or constraints, changing user expectations, and new use cases not anticipated during initial deployment. However, revisions should maintain ambition-targets should stretch systems toward excellence rather than rationalising mediocre performance.

8 Roadmap / Action Plan Outline

To ensure accountability and sustained momentum, the recommendations outlined in Section 6 must translate into a clear, phased execution plan. This roadmap delineates short-term (Foundation and Governance), medium-term (Technical Integration), and long-term (Scale-up and Sustainability) actions required by the Commission and Member States. The phased approach acknowledges the critical reality: only twelve months remain to meet the 2026 mandate.

Critical Note on Timeline Compression

The original DC4EU roadmap assumed action beginning in early 2025. This report is published in January 2026, compressing the available timeline by twelve months. Phases that were originally planned sequentially must now proceed in parallel where possible. This compression increases risk but remains technically feasible if political will and resources are immediately committed.

Phase 1: Foundation and Governance (January-March 2026)

This compressed three-month phase focuses on establishing essential legal and organizational mandates to transition from pilot status and mitigate immediate risks of fragmentation. The 2026 deployment deadline makes this phase non-negotiable.

Table 22: Phase 1 - Foundation and Governance

Action Pillar	Action Item	Owner	Completion Deadline	Critical Dependencies
Pillar 6.2 (Harmonised Governance)	Formal establishment of Top-Level Governance Board; board convened with terms of reference	EC, Member States	February 2026	Crucial for defining operational roles and preventing fragmented governance.
Pillar 6.3 (Sustainable Funding)	Secure multi-annual Production Funds; budget authority established for 2026-2031 cycle	EC (DG BUDG, DG Digital), Member States	March 2026	Budget negotiations concluded; funding commitments secured
Pillar 6.1 (Legal Clarity)	Legal Harmonisation Task Force established; common interpretative guidance drafted	EC Legal Services, Member States	March 2026	Task force operational by January; guidance ready for publication
Pillar 6.1 (Legal Clarity)	Verifier liability framework published	Legal Harmonisation Task Force	March 2026	Depends on guidance completion
Pillar 6.2 (Monitoring Framework)	KPI monitoring framework established; Section 7 metrics baselined	Governance Board, EC	March 2026	Ensures accountability and immediate measurement of implementation milestones.

Rationale and Critical Path

Governance establishment is crucial for preventing fragmented approaches as Member States rush toward the December 2026 deadline. Without top-level coordination operational by February, each Member State will proceed independently based on divergent interpretations, creating interoperability problems that become exponentially harder to resolve after systems are deployed.

Funding security by March 2026 prevents further institutional capacity loss. DC4EU funding ended July 2025; institutions have already experienced six months of uncertainty. Additional delay will result in irreversible loss of trained personnel and technical capabilities built over three years of piloting.

Legal clarity by March 2026 enables institutions to proceed with deployment confidence. Without authoritative guidance on credential equivalence and verifier liability, institutions will implement defensive practices rejecting valid foreign credentials, undermining cross-border recognition.

Phase 1 Success Criteria:

- Governance Board holds first meeting and publishes initial decisions
- Production Funds budget authority secured with multi-annual commitment
- Common interpretative guidance and verifier liability framework published
- KPI monitoring framework operational with baseline data collection

Phase 2: Technical Integration and Policy Finalisation (April-June 2026)

This three-month phase translates legal mandates into technical reality, addressing structural ARF and interoperability challenges. Actions proceed in parallel with Phase 1 where possible to compress timeline.

Table 23: Phase 2 - Technical Integration and Policy Finalisation

Action Pillar	Action Item	Owner	Completion Deadline	Critical Dependencies
Pillar 6.4 (Architectural Interoperability)	Deploy European Harmonisation Layer to production; standardised schemas and interoperability services operational	Technical WGs, Member States	June 2026	Development work began Q4 2025; testing completed May 2026
Pillar 6.4 (Architectural Interoperability)	Reference implementations and integration toolkits released as open source	Technical WGs	June 2026	Development completed; documentation finalised
Pillar 6.1 (Legal Clarity)	Finalise enforceable verifier policies; enforcement mechanism operational	Governance Board, EC	June 2026	Common guidance published (Phase 1); enforcement procedures defined
Pillar 6.4 (ARF Evolution)	Update ARF to resolve private sector exclusion gap; integrate private sector verifier requirements	Governance Board, EC	June 2026	Depends on governance board operational status
Pillar 6.5 (Citizen Trust)	Develop user acceptance testing protocols; train independent evaluators	Governance Board, Member States	June 2026	Testing scenarios defined; evaluator training completed

Rationale and Critical Path

The European Harmonisation Layer must be operational by June 2026 to provide institutions with the integration support needed for summer/fall deployment. Without this infrastructure, institutions face prohibitive integration costs (€250K-500K documented in Section 5.2), making comprehensive coverage economically infeasible for smaller public bodies.

Reference implementations and toolkits by June 2026 enable institutions beginning deployment in Q3 2026 to leverage reusable components rather than building everything from scratch. The seventy to eighty percent cost reduction documented in Section 6.4 depends on this tooling being available before major deployment efforts begin.

Enforceable verifier policies by June 2026 establish clear consequences for persistent non-compliance, ensuring that legal guidance published in Phase 1 translates into actual practice rather than remaining merely advisory.

ARF update addressing private sector exclusion by June 2026 is essential for mass adoption. The EUDI Wallet provides limited citizen value if it functions only for the small fraction of digital life involving government services while remaining irrelevant to commercial transactions that constitute the majority of online activity.

User acceptance testing protocols by June 2026 enable validation that systems being deployed actually work for citizens, not just for technical experts. The seventy-five percent independent task completion target specified in Section 7.2 requires rigorous testing methodology developed and validated before deployment begins.

Phase 2 Success Criteria:

- European Harmonisation Layer operational with documented cost reduction for early implementers
- Integration toolkits available as open source with active download/usage
- Enforcement mechanism operational with a reporting process accessible to citizens and institutions
- ARF updated to include private sector requirements
- User acceptance testing protocols validated through pilot testing

Phase 3: Scale-up and Capacity Building (July-December 2026)

This six-month phase represents the final push to meet the December 2026 mandate. Focus shifts to Member State deployment, citizen adoption, and ensuring user experience quality. Many actions proceed in parallel to compress timeline.

Table 24: Phase 3 - Scale-up and Deployment

Action Pillar	Action Item	Owner	Completion Deadline	Critical Dependencies
Pillar 6.5 (Citizen Trust)	Enforce User-First Design; mandatory user acceptance testing for all deployments	Member States, Wallet Providers, Verifiers	Ongoing (testing before deployment approval)	Testing protocols from Phase 2; independent evaluators are ready
Pillar 6.3 (Sustainable Funding)	Production Funds disbursed to institutions; funding agreements signed and operational	EC, Member States	July 2026	Budget authority from Phase 1; allocation formula applied
All Member States	Deploy functional EUDI Wallets; all 27 Member States meet minimum compliance	Member States	December 2026	Harmonisation Layer operational; tooling available; funding secured
Pillar 6.5 (Citizen Trust)	Launch EU-wide awareness campaigns; citizen education on wallet usage and benefits	Member States, EC	September 2026	Wallets deployed in sufficient Member States to justify campaigns

Pillar 6.4 (Architectural Interoperability)	Achieve 80% of Member States with cross-sectoral interoperability (credentials work across Education, Social Security, Healthcare)	Member States, Sectoral Authorities	December 2026 (initial target)	Extended to Dec 2027 per Section 7.1
Governance Board	Continuous compliance monitoring; publish first quarterly progress report against Section 7 KPIs	Governance Board	October 2026	KPI monitoring framework operational; sufficient deployment data available

Rationale and Critical Path

User-first design enforcement throughout deployment ensures systems meet the seventy-five percent independent success rate target. Testing must occur before deployment approval, preventing poor user experience from characterizing initial citizen interactions that shape long-term trust.

Production Funds disbursement by July 2026 provides institutions with financial security as they enter the intensive deployment phase. Funding certainty enables hiring staff, procuring infrastructure, and committing to deployment timelines without risk of resource constraints forcing delays.

All Member States deploying by December 2026 is the legal mandate. This represents the absolute deadline beyond which non-compliance becomes a regulatory violation. The roadmap's earlier phases exist to make this deadline achievable rather than aspirational.

Awareness campaigns launching September 2026 ensure citizens know about wallet availability and understand benefits. Campaigns too early (before sufficient deployment) create frustration; campaigns too late miss the critical adoption window when citizens are most open to trying new systems.

Cross-sectoral interoperability by December 2026 is aspirational given timeline compression; the more realistic target of eighty percent of Member States by December 2027 (specified in Section 7.1) acknowledges that deep sectoral integration requires time beyond minimum compliance.

Governance Board quarterly reporting beginning October 2026 establishes accountability and transparency. The first report provides early warning of problems requiring intervention before they become systemic failures.

Phase 4: Sustainability and Innovation (2027 Onward)

This ongoing phase ensures long-term institutionalization and prepares the ecosystem for continuous evolution. Actions transition from deployment focus to operational excellence and innovation.

Table 25: Phase 4 - Sustainability and Innovation

Action Pillar Focus	Action Item	Owner	Timeline	Purpose
Pillar 6.3 (Sustainable Funding)	Implement alternative sustainability models beyond public funding; explore business models for private sector value-added services	Governance Board, Industry	2027-2028	Ensure financial health beyond initial EU investment; enable innovation

Pillar 6.2 & 6.4 (Global Alignment)	Design framework for strategic international (alignment with UNCITRAL, other global standards bodies)	EC, Technical WGs	2027-2029	Ensure EUDI Wallet remains globally relevant; support EU citizens travelling outside Europe
Pillar 6.4 (Innovation)	Prioritise investment in composite credentials (e.g., 'Labour Card' combining education, professional qualifications, and work authorisation)	Governance Board, Sectoral Authorities	2027-2030	Enable advanced use cases beyond simple credential presentation
Pillar 6.2 (Sustained Governance)	Governance Board ensures sustained political momentum; dynamically updates trusted lists, data models, ARF specifications	Governance Board	Ongoing	Prevent stagnation; respond to emerging requirements and security threats
All Pillars	Achieve quantitative targets from Section 7.1 (40% citizen adoption, 95% verification success, 60% processing time reduction)	All Actors	2027-2029	Demonstrate system delivers promised value; justify continued investment
Pillar 6.5 (User Experience)	Continuous user experience monitoring and improvement; regular testing; feedback mechanisms	Member States, Wallet Providers	Ongoing	Maintain quality as systems evolve; prevent degradation

Rationale and Long-Term Vision

Alternative sustainability models beyond public funding become necessary as the ecosystem matures. Private sector services built on EUDI Wallet infrastructure (identity verification for banking, age verification for e-commerce, professional credential verification for hiring) can generate revenue supporting ongoing operation while providing value-added services beyond basic public sector use cases.

International interoperability ensures European citizens travelling globally can use their EUDI Wallets, and international partners can verify European credentials. Alignment with UNCITRAL (United Nations Commission on International Trade Law) and other global standards bodies positions Europe as leader rather than follower in digital identity evolution.

Composite credentials represent natural evolution beyond simple single-attribute attestations. A worker needing to prove eligibility for cross-border employment currently requires multiple credentials (educational diploma, professional license, work authorisation, social security coverage). A composite "Labour Mobility Card" combining these into a single presentation simplifies user experience while maintaining selective disclosure (worker proves employment eligibility without revealing unrelated details like specific grades or medical information).

Sustained governance prevents the gradual drift and fragmentation that often affects complex systems over time. The Governance Board must maintain active oversight ensuring technical evolution remains coordinated, security standards keep pace with emerging threats, and Member States continue meeting compliance obligations rather than allowing gradual non-compliance as initial deployment urgency fades.

Achieving Section 7.1 quantitative targets validates that the system delivers promised value. Forty percent citizen adoption within three years demonstrates genuine utility rather than forced compliance. Ninety-five percent verification success and sixty percent processing time reduction prove operational excellence. These targets justify continued investment and political support.

Continuous user experience monitoring ensures quality maintenance. Initial deployment quality can degrade as systems evolve, staff turnover occurs, and institutional priorities shift. Regular

testing, user satisfaction surveys, and feedback mechanisms enable early detection of problems before they become systemic.

Phase 4 Success Criteria:

- Alternative revenue models operational supplementing public funding
- International interoperability frameworks established with key partner countries/regions
- At least three composite credential types piloted and deployed
- Governance Board demonstrates sustained effectiveness through regular decision-making and compliance enforcement
- Section 7.1 quantitative targets achieved on schedule
- User satisfaction scores maintain or improve from the initial deployment baseline

Roadmap Governance and Adaptation

Accountability Mechanisms

The Governance Board established in Phase 1 holds primary accountability for roadmap execution. Quarterly progress reviews assess completion of phase milestones, identify delays requiring intervention, recommend resource reallocation addressing bottlenecks, and escalate systemic problems to the political level when necessary.

Risk Management

The compressed timeline creates elevated risks: timeline slippage in early phases cascades to later phases with no buffer; institutional capacity already lost from the DC4EU funding gap may not be recoverable; political will may waver if early complications emerge; and technical challenges may prove more difficult than anticipated. Mitigation strategies include parallel execution where dependencies allow, dedicated troubleshooting resources for early problem identification, transparent progress reporting enabling rapid intervention, and political-level sponsorship maintaining momentum through challenges.

Adaptive Execution

While the roadmap provides structure, operational reality will require adaptation. The monthly steering committee reviews assess whether timeline assumptions remain valid, identify emerging opportunities or constraints requiring plan modification, approve necessary deviations from planned sequence, and maintain documentation of decisions for accountability and learning.

Integration with Section 7 KPIs

This roadmap directly supports achieving Section 7 metrics. Phase 1 actions enable Legal Clarity and Governance milestones. Phase 2 actions deliver Architectural Interoperability and User Experience capabilities. Phase 3 actions drive Member State Compliance and initial adoption metrics. Phase 4 actions achieve long-term quantitative targets. The Governance Board's quarterly reporting integrates roadmap progress with KPI achievement, providing a unified accountability framework.

9 Conclusion

This study provides comprehensive examination of digital identity's future in Europe through empirical evidence from real-world implementation. By successfully piloting the European Digital Identity Wallet across 101 institutions in 25 countries, DC4EU demonstrated that the vision works. The project issued and verified high-assurance credentials - digital diplomas, professional qualification in regulated domains,, health insurance cards, and social security documents - across borders, establishing the EUDI Wallet as Europe's foundational digital trust instrument.

Technical Viability Proven

DC4EU confirmed that real-world implementation demands simultaneous efforts in legal harmonization, governance transformation, and cultural shifts in how institutions manage identity data. The project achieved critical operational successes:

Technical Feasibility: Successful cross-border issuance and verification of high-assurance credentials including QEAAs and PuB-EAAs (EHIC, Digital Diplomas) demonstrated that protocols work, and cryptographic verification provides promised assurance. eIDAS establishes binding recognition obligations, whose effective application depends on correct interpretation and enforcement.

Pluralistic Coexistence Strategy: The discovery that Europe's institutional diversity requires embracing multiple approaches emerged from implementation experience, not predetermined design. The coexistence of three distinct trust frameworks-EBSI for new public sector credentials, OpenID Federation for federated academic settings and verification, and traditional PKI/eIDAS for legacy credentials-reflects necessary architectural flexibility aligned with the EU's diverse institutional landscape. This complexity is the non-negotiable path to institutional adoption.

Each trust infrastructure contributes essential capabilities. EBSI provides permanent verifiable records and governance frameworks across countries and sectors. OpenID Federation enables integration with established networks like eduGAIN while enforcing privacy through selective disclosure. PKI/eIDAS continues anchoring credentials with decades of proven reliability. No single approach can serve all of Europe; the integrated architecture respects both institutional realities and future innovation.

Systematic Barriers Blocking Deployment

Despite proven technical viability, five systematic barriers at the EU level now prevent transition from pilot success to production deployment:

Unsustainable Funding: Project-based grants cannot sustain operational infrastructure. DC4EU funding ended in July 2025, creating immediate capacity loss. Survey data revealed that sixty percent of small institutions cannot sustain beyond twelve to eighteen months without guaranteed multi-annual funding; thirty-five percent already lost key staff to more secure positions.

Legal Fragmentation: Divergent national interpretations of GDPR and eIDAS create silos threatening cross-border recognition. Verifiers refuse legally valid credentials based on technical issuance source despite equivalent assurance-fifteen percent of pilot verification failures stemmed from institutional uncertainty, not technical errors.

ARF Gaps: The Architecture Reference Framework provides a strong technical blueprint but requires evolution into more prescriptive, enforceable guidance. Critical gaps include private sector exclusion limiting utility, absence of a funded European Harmonisation Layer for metadata translation, and integration costs (€250K-500K per institution) prohibitive for smaller agencies.

Governance Fragmentation: No politically mandated authority exists to enforce common standards. Forty percent of pilot institutions reported unclear guidance about responsibilities.

Sectoral autonomy without coordination creates silos where credentials work within sectors but not across them.

User Experience Failures: Twenty-five percent of pilot transactions required manual intervention. Seventy percent of citizens stated they would revert to paper if digital verification "didn't just work." The "data courier" risk-forcing citizens to manually transport information between systems-directly undermines the wallet's value proposition.

From Blueprint to Political Execution

The EUDI Wallet must fundamentally reshape how identity is used in society, not merely digitise existing documents. DC4EU laid a strong technical foundation proving viability. The challenge is no longer technical: it is political execution at scale.

The Timeline Imperative: Less than twelve months remain until the December 2026 mandate. Member States must deploy functional wallets within this compressed timeframe. Success demands immediate action across Five Core Action Pillars:

Legal Clarity (Q1 2026): Establish legal certainty through common interpretative guidance guaranteeing equivalence across QEAAs, PuB-EAAs, and properly accredited non-qualified EAAs. Publish enforceable verifier liability policies preventing credential discrimination based on technical issuance source.

Harmonised Governance (Q1 2026): Create top-level Governance Board with political authority to prevent fragmented national approaches. The board must enforce metadata standards, resolve sectoral conflicts, and maintain ARF evolution – *not* merely advise.

Sustainable Funding (Q1 2026): Introduce multi-annual Production Funds (€250-500M annually) providing predictable operational financing beyond project cycles. Support both core European infrastructure and institutional capacity building across Member States.

Architectural Interoperability (Mid-2026): Deploy European Harmonisation Layer reducing integration costs seventy to eighty percent through schema translation, governance mapping, and unified verification APIs. Provide reference implementations and toolkits as open-source software.

Citizen Trust (Mid-2026): Enforce user-first design principles eliminating data courier scenarios. Mandate seventy-five percent independent task completion rate through rigorous user acceptance testing before deployment approval.

Critical Urgency

Three actions must occur in Q1 2026 or the mandate fails: securing Production Funds preventing further capacity loss, establishing Governance Board coordinating Member State approaches, and publishing legal guidance enabling confident deployment. Two additional actions must complete by mid-2026: deploying Harmonisation Layer enabling cost-effective integration and enforcing user-first design ensuring quality experience.

DC4EU funding ended July 2025; institutions have experienced six months of uncertainty causing documented capacity loss. Additional delay produces irreversible consequences as trained personnel depart, institutional knowledge dissipates, and systems enter maintenance-only mode. The six-month gap already incurred makes the December 2026 deadline extremely challenging. Further delay makes it impossible.

Europe's Choice

Europe possesses the technical blueprint. The system works-credentials can be issued, verified across borders, and used securely with privacy protection. The architecture accommodates

institutional diversity while maintaining interoperability. The legal framework supports automatic cross-border recognition. What remains is execution.

The Commission must immediately launch a dedicated Production Funding Call for execution and institutionalization. Member States must commit political will and resources to coordinated deployment. The Governance Board must be operational by February 2026. Legal guidance must publish by March 2026. The Harmonisation Layer must deploy by June 2026. These are not aspirational goals: they are prerequisites for meeting the legal mandate twelve months away.

The alternative to immediate, coordinated action is clear: fragmentation into incompatible national implementations that fail to deliver cross-border interoperability, institutional atrophy as capabilities built over three years of piloting dissipate, citizen distrust as poor user experience drives abandonment, and ultimately failure to meet the 2026 mandate with broader consequences for European digital sovereignty ambitions.

DC4EU demonstrated that the EUDI Wallet can work. Whether it will work at scale across Europe depends entirely on decisions made in the next three months. The technical foundation is ready. The question is whether Europe is ready to execute.

Further Reading

The findings and policy recommendations in this report are validated by the detailed technical specifications, legal analyses, and empirical results of the DC4EU project. For further detail on the architecture, testing, and implementation outcomes, consult the following official deliverables and published papers.

Published Papers and Articles (Strategic and Legal Context)

These publications provide the strategic, legal, and operational context that underpins the policy recommendations made in Sections 5 and 6.

Ariño-Martin, L.-A. (2025, July). *eduGAIN: Structure, governance and sovereignty in the European academic federated identity ecosystem*. DC4EU. https://www.dc4eu.eu/wp-content/uploads/2025/11/Paper-15-eduGAIN_Full_Report_DC4EU.pdf

Ariño-Martin, L.-A., Alamillo-Domingo, I., & BotaPorta, L. (2025). *A non-qualified trust service provider model for higher education: Integrating legal compliance and technical architecture for digital credentials*. DC4EU. https://www.dc4eu.eu/wp-content/uploads/2025/09/A-non-qualified-trust-service-provider-model.pdf

Bauer, G., & Alamillo, I. (2025, May 30). *Attestation of attributes issued by public bodies: A citizen-centric trust model for the EUDI Wallet*. SSRN. https://doi.org/10.2139/ssrn.5398805

Bauer, G., Gabel, H., Hilmar, K., Ilsøe, L., & Kaaber, C. (2025, August 20). *Enabling cross-border social security through the European Digital Identity Framework*. SSRN. https://doi.org/10.2139/ssrn.5398731

den Hertog, P., van Dijk, N., & Wierenga, K. (2025, July). *A trusted foundation for the EUDI Wallet in research and education: Why eduGAIN and OpenID Federation matter*. DC4EU. https://gist.github.com/pauldenhertog/5bebc3992e0ce831122ac3f37c7936ad

Flanagan, H., & Johansson, L. (2025, August). *Deployability first: Making age verification work at Internet scale* [Conference presentation]. IAB/W3C Workshop on Age-Based Restrictions on Content Access. https://datatracker.ietf.org/doc/slides-agews-paper-deployability-first-making-age-verification-work-at-internet-scale/

Project Deliverables (Technical and Testing Evidence)

These deliverables provide empirical evidence supporting claims of technical viability, interoperability, and successful pilot user journeys discussed in Sections 3 and 4.

Bauer, G., Hilmar, K., Damdinbazar, K., Ilsøe, L., Friedl, P., Alamillo-Domingo, I., & Kaaber, C. (2025, July 29). *Deployment, testing and piloting scenarios results library* (DC4EU, Work Package 6, Task D6.2, Deliverable v1.1) [Report]. DVSV. https://www.dc4eu.eu/wp-content/uploads/2025/11/DC4EU-WP6_D6.2_DTPSRL-1.pdf

DC4EU. (2025). *DC4EU WP5 D5.2 deployment and testing scenarios results library* (Grant Agreement No. 101102611). https://www.dc4eu.eu/wp-content/uploads/2025/11/DC4EU_WP5_D5.2-Deployment-and-Testing-Scenarios-Results-Library.pdf

Fourtounis, G., Mergoupis-Anagnou, F., & Bekakou, A. (2025). *D5.5 - A prototype demonstrating the issuance and verification workflows* (DC4EU deliverable WP5, Milestone 38, Rev. v1.3). GRNET. https://www.dc4eu.eu/wp-content/uploads/2025/11/DC4EU_WP5_D5.5-A-prototype-demonstrating-the-issuance-and-verification-workflows.pdf

Hilmar, K., Bauer, G., & Beda, K. (2025). *DC4EU WP6 user journeys* (Deliverable of the Digital Credentials for Europe project, Grant Agreement No. 101102611). DC4EU. https://www.dc4eu.eu/wp-content/uploads/2025/08/DC4EU_WP6_User_Journeys.pdf