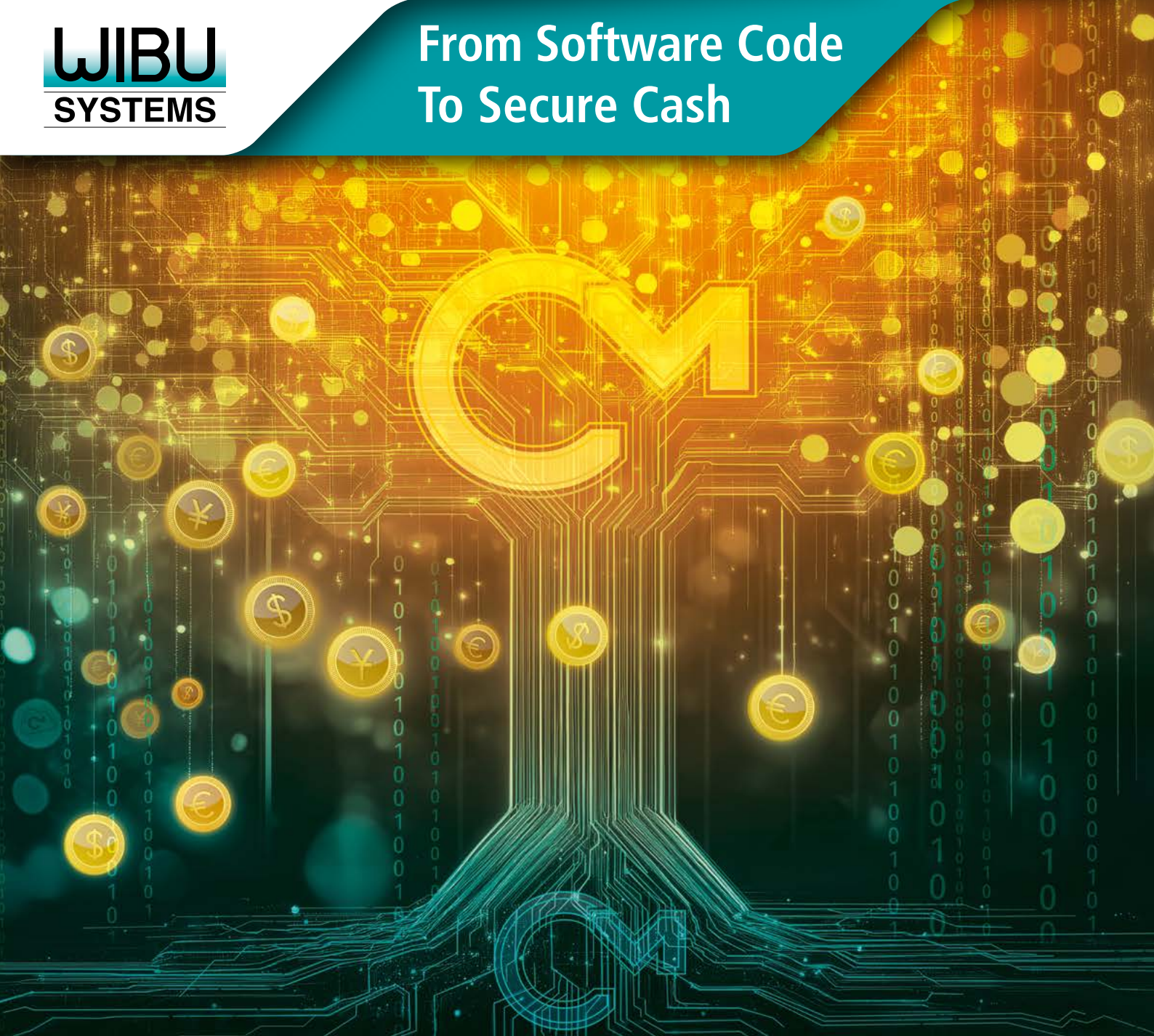

THE QUANTUM SPACE
TQS EXECUTIVE INTELLIGENCE
IDENTITIES AT SCALE
EUDI Wallets, National Pilots and the Road to Production
FEBRUARY 2026
Digital identity is no longer a policy experiment. Identities at Scale explores what happens when Europe's wallet ambitions collide with real-world scale, regulation, and security — and why the next phase will be won or lost in the details.

WIBU SYSTEMS

From Software Code To Secure Cash



Turn your software into a thriving revenue generator with CodeMeter.

- **Flexible Monetization:** Adaptable licensing models for all market demands
- **Robust IP Protection:** Innovative encryption and integrity protection methods
- **Effortless Compatibility:** Smooth integration into diverse platforms
- **Future-Proof Solutions:** Designed to evolve alongside your business needs

With CodeMeter, your software grows stronger roots and flourishes.

sales@wibu.com
www.wibu.com

Start now and request your CodeMeter SDK
wibu.com/sdk

IDENTITIES AT SCALE

EUDI Wallets, National Pilots, and the Road to Production

The Quantum Space
February 2026

Table of Contents

Executive Summary

Europe's move toward a European Digital Identity (EUDI) Wallet represents one of the most ambitious attempts to establish digital identity as shared public infrastructure rather than as a proprietary platform or isolated national service. Enabled by the revision of the electronic Identification, Authentication and Trust Services Regulation (eIDAS 2.0), EUDI seeks to provide citizens and organisations with secure, interoperable digital identity capabilities that function across borders and sectors.

After several years of policy development and large-scale pilot programmes, EUDI has entered a decisive phase. Technical feasibility has largely been demonstrated. Wallet architectures exist. Cross-border credential exchange is possible. Yet a growing gap has emerged between pilot success and production readiness. The central challenge facing EUDI is no longer whether digital identity wallets can work, but whether identity systems can operate reliably at scale.

This whitepaper argues that digital identity at population and enterprise scale is shaped less by user experience than by governance, liability, lifecycle management, and long-term trust assumptions. These factors are difficult to surface in pilot environments, which are inherently bounded and optimised for learning rather than durability. As a result, pilot outcomes should be interpreted as indicators of plausibility, not proof of readiness.

An examination of EU-level Large-Scale Pilots alongside detailed national case studies highlights the structural diversity of Europe's identity landscape. Germany's federal governance model prioritises legal certainty and high assurance, favouring durability over speed. The Nordic countries demonstrate how mature trust environments enable faster experimentation and strong public–private collaboration. The Netherlands illustrates a pragmatic, service-led approach that bridges policy ambition and operational reality. The Baltic states show the power of digital-first governance, while also underscoring the limits of extrapolating small-state success to continental scale.

Together, these cases reinforce a central conclusion: EUDI will not arrive uniformly across Europe. Adoption will be uneven by design, shaped by national governance models, sectoral priorities, and risk tolerance. This diversity does not undermine the initiative; it defines it. The task ahead is to manage variation without fragmenting trust.

For enterprises, EUDI introduces both opportunity and uncertainty. It will not replace existing identity and access management systems, nor will it function as a universal login mechanism. Instead, organisations are likely to adopt EUDI selectively, integrating wallet-based credentials where they reduce cost, improve assurance, or support cross-border interaction. Liability clarity, operational integration, and sustainable governance will determine the pace and depth of enterprise engagement.

The transition from pilots to production represents the critical inflection point. Moving forward requires more than technical refinement. It demands clear operational ownership, defined liability frameworks, sustainable funding models, and governance structures capable of scaling with adoption. Without these commitments, EUDI risks remaining a permanent pilot programme rather than becoming dependable infrastructure.

Success for EUDI should not be measured by rapid uptake or uniform deployment. At infrastructure scale, success is gradual, often invisible, and assessed over years rather than programme cycles. A successful EUDI ecosystem will be one in which identity functions quietly and predictably, supporting economic activity and public services without drawing attention to itself.

If achieved, Europe will have demonstrated that digital identity can operate as interoperable, rights-respecting public infrastructure at continental scale. That achievement would extend beyond Europe itself, offering a credible alternative to platform-centric identity models and shaping global expectations of how trust can be built and sustained in the digital age.

1. From Regulation to Reality: Why EUDI Exists

The European Digital Identity (EUDI) initiative is not the result of a single policy decision, nor is it a sudden response to technological change. It represents the culmination of more than a decade of experimentation, fragmentation, and gradual realisation that Europe's digital identity landscape could not scale in its existing form.

1.1 The Limits of the First eIDAS Era

The original electronic Identification, Authentication and Trust Services Regulation (eIDAS), adopted in 2014, established a legal framework for electronic identification and trust services across the European Union. Its core objective was to enable cross-border recognition of nationally issued electronic identification schemes for access to public services.

In practice, eIDAS achieved only partial success. While a number of Member States notified national eID schemes, uptake varied widely. Integration was complex, incentives for private-sector adoption were weak, and usage remained largely confined to public administration use cases. Rather than creating a unified European identity layer, eIDAS reinforced a patchwork of nationally anchored systems connected by regulatory obligation rather than operational coherence.

The result was a European digital identity environment that worked in principle but struggled in practice. Citizens encountered inconsistent experiences across borders. Service providers faced high integration costs for limited reach. Enterprises largely continued to rely on existing identity and authentication mechanisms, including bank-issued credentials, proprietary platforms, or global technology providers.

1.2 Structural Pressures for Change

By the late 2010s, several structural pressures converged to expose the limitations of this model. Cross-border digital services increased rapidly, particularly in areas such as finance, mobility, education, and platform-based work. At the same time, reliance on non-European identity providers raised concerns around strategic autonomy, data protection, and regulatory alignment.

The growth of platform ecosystems also highlighted a deeper issue: identity was no longer simply a means of authentication. It had become a prerequisite for trusted digital interaction, attribute sharing, and compliance-driven verification. Existing models, built around static identifiers and narrow use cases, were ill-suited to these demands.

In parallel, regulatory developments in areas such as anti-money laundering, data protection, and cybersecurity increased pressure on organisations to improve identity assurance while minimising data exposure. This tension — between stronger verification and greater user control — became a central design challenge for any future European identity framework.

1.3 eIDAS 2.0 and the Wallet Paradigm

The revision of eIDAS, commonly referred to as eIDAS 2.0, represents a deliberate shift in approach. Rather than focusing solely on the mutual recognition of national eID schemes, the revised framework introduces the concept of a European Digital Identity Wallet as a common interaction layer.

Under this model, individuals and organisations are expected to use wallets to store and present verifiable credentials issued by trusted sources. These credentials may include identity attributes, professional qualifications, licences, or other attestations relevant to specific use cases. The wallet becomes the interface through which trust is exercised, rather than the identity provider itself.

This shift reframes digital identity from a monolithic service into a modular ecosystem composed of issuers, holders, verifiers, trust frameworks, and governance structures. While wallets are the most visible element of this ecosystem, they are not its defining feature. The core challenge lies in standardising trust relationships across borders while preserving national sovereignty over identity issuance.

1.4 Identity as Infrastructure

A central premise of the EUDI initiative is that digital identity should be treated as infrastructure rather than as an application or product. Infrastructure systems must operate reliably at national and continental scale, integrate with legacy environments, accommodate regulatory diversity, and remain viable over long time horizons.

In this context, the challenges facing EUDI extend well beyond wallet usability or cryptographic design. They include governance models, liability allocation, lifecycle management, interoperability between sectors, and the alignment of public and private interests. Many of these challenges only emerge when systems are tested beyond controlled pilot environments.

1.5 From Policy Intent to Operational Reality

The introduction of EUDI reflects a recognition that Europe's digital economy requires a more coherent identity foundation. However, regulatory intent does not automatically translate into operational reality. The transition from framework to functioning infrastructure is where most large-scale digital identity initiatives encounter friction.

As EUDI moves from specification to implementation, its success will depend less on architectural elegance than on its ability to absorb complexity without collapsing under it. This requires realistic assumptions about adoption, selective deployment across sectors, and an acceptance of uneven progress across Member States.

The following sections examine how Europe has begun to test these assumptions through large-scale pilot programmes, what these pilots reveal about the path ahead, and why the journey from experimentation to production remains the defining challenge for the European Digital Identity initiative.

Sources and References

- European Commission, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
- European Commission, Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (eIDAS 2.0).
- European Commission, 2030 Digital Compass: the European way for the Digital Decade.
- ENISA, Trust Services and Digital Identity in the EU.
- European Data Protection Board (EDPB), guidance and opinions on digital identity and attribute sharing.

2. The Pilot Landscape: Where Europe Really Stands

As the European Digital Identity (EUDI) framework moves from regulation into implementation, large-scale pilot programmes have become the primary lens through which progress is assessed. These pilots represent Europe's first sustained attempt to translate eIDAS 2.0 from legal intent into operational reality. They are not proof of readiness, but they are valuable indicators of direction, constraint, and divergence.

Examining the pilot landscape reveals a fundamental truth: EUDI is not advancing along a single, uniform path. Instead, it is unfolding through a series of nationally shaped experiments, each reflecting distinct governance models, trust assumptions, and risk tolerances. Understanding where Europe "really stands" therefore requires looking beyond aggregate pilot success and into how different Member States interpret, adapt, and stress-test the same framework under very different conditions.

2.1 Reading the Pilots: What National Case Studies Reveal

National case studies provide a grounded way to interpret the pilot phase. While EU-level programs define common architectures and interoperability goals, it is within Member States that governance decisions, institutional constraints, and real operational trade-offs surface. The same technical framework produces very different outcomes when filtered through federal versus centralized systems, high-assurance versus risk-proportionate models, and public-sector-led versus market-driven approaches.
The following case studies are not intended as rankings or templates. Instead, they illustrate how EUDI is being shaped in practice — what appears to be working, what remains unresolved, and why progress is necessarily uneven. Together, they show that variation is not a failure of the European Digital Identity initiative, but one of its defining structural realities.

Country Case Study: Germany

Germany occupies a pivotal position in the European Digital Identity (EUDI) landscape. As Europe's largest economy and a federal state with complex

institutional structures, Germany's approach to EUDI illustrates both the opportunities and the constraints inherent in deploying digital identity at scale.

Governance and Institutional Structure

Responsibility for digital identity in Germany is distributed across federal ministries, Länder authorities, and specialized agencies. The Federal Ministry of the Interior and Community (BMI) plays a central coordinating role, while implementation and service delivery often sit with Länder-level bodies and affiliated institutions. This federal structure has historically slowed nationwide digital initiatives, but it also enforces a high bar for legal robustness and constitutional alignment.

Within the EUDI context, Germany's participation in multiple EU Large-Scale Pilots reflects a cautious but committed strategy. Rather than pursuing a single, monolithic wallet model, Germany has explored approaches that balance federal coordination with delegated or sector-specific implementations.

Pilot Participation and Use Cases

Germany is involved in several EUDI Large-Scale Pilots, including initiatives focused on public administration services, professional credentials, and cross-border identification. Use cases under examination range from access to government portals and business services to qualification and status verification in regulated professions.

A notable characteristic of the German pilots is their emphasis on compliance, assurance, and legal certainty. Pilot designs prioritise alignment with existing identity frameworks, data protection requirements, and national security considerations. While this approach can limit speed, it increases the likelihood that successful pilot outcomes can transition into production environments.

Wallet Model and Trust Anchors

Germany's wallet strategy reflects its broader digital identity philosophy. Rather than positioning the wallet as a standalone consumer application, German pilots treat it as an interface layered on top of established trust anchors. These include state-issued identity documents, hardware-backed security elements, and certified trust services.

Hardware roots of trust play a significant role in German thinking around EUDI. This emphasis aligns with the country's long-standing reliance on secure elements in national identity cards and regulated environments. As a result, German pilots tend to favour higher-assurance configurations, even where this introduces additional complexity.

What Appears to Be Working

Germany's strength lies in its ability to integrate EUDI concepts into existing legal and institutional frameworks. Pilot outcomes demonstrate that high-assurance digital identity interactions can be aligned with European interoperability requirements without undermining national controls. The focus on compliance and governance positions Germany well for regulated and enterprise-heavy use cases.

What Remains Unresolved

The same factors that underpin Germany's robustness also present challenges. Federal complexity complicates nationwide rollout, and coordination across Länder introduces variability in implementation timelines. Questions around operational ownership, funding models, and cross-sector adoption remain open.

Germany's experience suggests that EUDI deployment at scale will favour durability over speed. For enterprises, this signals a stable but gradual integration path, particularly in regulated sectors where legal certainty outweighs time-to-market.

Country Case Study: Nordics (Norway, Finland, Sweden)

The Nordic countries represent a markedly different trajectory within the European Digital Identity landscape. Long recognised for high levels of digital trust, mature national eID systems, and strong public–private collaboration, the Nordics approach EUDI from a position of operational confidence rather than institutional caution.

Governance and Trust Environment

Nordic digital identity systems benefit from relatively centralised governance models, clear lines of accountability, and high public acceptance of digital public services. Bank-issued and state-backed electronic identities have been widely used for years across both public and private sectors, creating a culture in which digital identity is already embedded in daily life.

This maturity shapes Nordic engagement with EUDI. Rather than treating the European Digital Identity Wallet as a foundational capability, Nordic actors view it as an extension layer — a mechanism to project existing trust frameworks across borders.

NOBID and Cross-Border Ambition

The Nordic-Baltic EUDI Large-Scale Pilot (NOBID) exemplifies this outward-facing approach. Focused on cross-border use cases, NOBID explores how trusted national credentials can be reused seamlessly across jurisdictions, particularly in areas such as payments-adjacent identity, access to services, and professional mobility.

A defining feature of the Nordic pilots is their emphasis on real-world applicability. Use cases are chosen for immediate relevance, and private-sector actors play an active role in shaping requirements. This contrasts with pilots that prioritise institutional alignment over market pull.

Wallet Models and Operational Flexibility

Nordic wallet strategies tend to emphasise flexibility over uniformity. Rather than enforcing a single state-controlled wallet, pilots accommodate multiple wallet implementations aligned with common trust frameworks. This pluralistic model reflects confidence in governance mechanisms rather than concern over fragmentation.

Software-based solutions are more prominent in Nordic pilots than in higher-assurance environments such as Germany. This reflects different risk assumptions, smaller populations, and long-standing experience managing digital trust without pervasive hardware anchoring.

What Appears to Be Working

The Nordic approach demonstrates that strong trust foundations enable faster experimentation and smoother public–private collaboration. Cross-sector reuse of credentials is more readily achievable, and user acceptance is high. For enterprises, this environment lowers barriers to integration and accelerates learning cycles.

What Remains Unresolved

Nordic success does not automatically translate to pan-European scalability. Smaller populations, homogeneous trust cultures, and simpler governance structures limit direct extrapolation. Questions remain around how Nordic-style flexibility performs under the legal, cultural, and demographic diversity of larger Member States.

The Nordic case highlights both the potential and the limits of maturity-led deployment. It suggests that EUDI can move quickly where trust already exists — but also underscores why European-wide rollout cannot assume Nordic conditions as the norm.

Country Case Study: Netherlands

The Netherlands occupies a pragmatic middle ground in the European Digital Identity landscape. Neither as institutionally complex as Germany nor as culturally trust-saturated as the Nordics, the Dutch approach to EUDI is characterised by service orientation, practical governance, and a long-standing emphasis on usability within clearly defined trust frameworks.

Governance and Policy Context

Digital identity in the Netherlands has historically been shaped by a balance between strong public-sector coordination and active private-sector participation. The Dutch government has invested heavily in digital public services, while maintaining a cautious stance toward centralised identity control. This has produced an ecosystem that favours clear rules, modular architectures, and incremental deployment.

Within the EUDI framework, the Netherlands approaches participation less as a constitutional exercise and more as a service delivery challenge. The focus is on how European identity capabilities can be integrated into existing public and private digital services without disrupting operational continuity.

Pilot Participation and Use Cases

The Netherlands is involved in multiple EUDI Large-Scale Pilots, with particular attention to public-sector access, business services, and attribute-based verification. Dutch pilots tend to prioritise use cases that are already familiar to citizens and enterprises, such as interaction with government portals, regulated service access, and professional credentials.

A defining characteristic of Dutch pilots is their emphasis on clarity and scope control. Rather than testing an expansive set of scenarios, pilots are structured around well-defined interactions that can realistically transition into production.

Wallet Strategy and Service Design

Dutch wallet strategies reflect the country's broader digital philosophy. Wallets are treated as service components rather than as symbolic national assets. Design choices emphasise interoperability, consent management, and integration with existing digital journeys.

Unlike approaches that prioritise either maximum assurance or maximum flexibility, the Dutch model seeks balance. Assurance levels are aligned with use-case requirements, and technical choices are evaluated through the lens of operational maintainability rather than theoretical capability.

What Appears to Be Working

The Netherlands demonstrates the value of pragmatic governance. By aligning EUDI experimentation closely with existing services, Dutch pilots reduce the gap between testing and deployment. This increases the likelihood that pilot outcomes can be operationalised without major redesign.

For enterprises, this environment offers predictability. Clear rules, stable interfaces, and realistic deployment assumptions lower integration risk and support gradual adoption.

What Remains Unresolved

The Dutch emphasis on pragmatism may limit ambition in areas that require more radical rethinking of identity models. Questions remain around how far existing service-centric approaches can stretch to accommodate cross-border complexity at scale.

The Netherlands case illustrates that successful EUDI deployment does not require extremes. It highlights the role of measured, service-driven integration as a viable path between high-assurance rigidity and rapid experimentation.

The European Digital Identity Wallet initiative has progressed beyond abstract policy intent into a phase of structured experimentation. Across Europe, large-scale pilot programmes are now testing technical architectures, governance models, and cross-border interactions. These pilots represent the first serious attempt to operationalise the principles set out in eIDAS 2.0.

However, pilots are not production systems. They are designed to explore feasibility, surface design questions, and reduce uncertainty — not to demonstrate readiness for mass deployment. Understanding what the current pilot landscape does and does not reveal is therefore essential to assessing Europe's true position on the road to scale.

Country Case Study: Baltics (Estonia, Latvia, Lithuania)

The Baltic states occupy a distinctive position in the European Digital Identity landscape. Often cited as digital pioneers, Estonia, Latvia, and Lithuania have built reputations for innovation, agility, and digital-first governance. Their engagement with EUDI reflects this heritage — but it also exposes the limits of extrapolating small-state success to continental scale.

Governance and Digital-First Foundations

The Baltic countries benefit from relatively centralised governance models, compact administrative structures, and strong political consensus around digital transformation. Estonia in particular has embedded digital identity deeply into public administration, business formation, healthcare, and civic interaction. Latvia and Lithuania, while following different trajectories, share similar commitments to digital public services and cross-border interoperability.

This environment allows Baltic authorities to experiment quickly and deploy changes with fewer institutional constraints than larger Member States. Decision-making cycles are shorter, and coordination between agencies is typically more direct. As a result, digital identity initiatives can move from concept to operation at a pace that is difficult to replicate elsewhere in Europe.

EUDI Engagement and Pilot Orientation

Within the EUDI framework, Baltic participation focuses on leveraging existing national digital identity capabilities in a European context. Pilots tend to emphasise interoperability, credential portability, and cross-border service access rather than foundational identity issuance.

Baltic actors approach EUDI less as a transformative reset and more as an opportunity to extend proven national models. This pragmatic stance allows pilots to demonstrate functionality rapidly, particularly in scenarios involving public services, business processes, and regional mobility.

Wallet Models and Trust Assumptions

Baltic wallet strategies are shaped by confidence in software-centric identity architectures. Long-standing reliance on digital certificates, central registries, and online services has fostered trust in software-based solutions supported by strong institutional controls.

Compared to higher-assurance environments, hardware roots of trust play a less dominant role in Baltic pilots. This reflects both risk assumptions and population scale. While effective domestically, this approach raises questions about portability to larger, more heterogeneous markets with different threat models and regulatory expectations.

What Appears to Be Working

The Baltic experience demonstrates the power of clarity and institutional alignment. Digital identity systems benefit when governance is simple, mandates are clear, and digital interaction is the default rather than the exception. Baltic pilots show that EUDI-aligned credentials can integrate smoothly into everyday services when foundational trust is already established.

For EUDI as a whole, the Baltics provide valuable insight into how identity ecosystems behave when friction is minimised and digital literacy is high.

What Remains Unresolved

The primary limitation of the Baltic model lies in scale and transferability. Small populations, high digital literacy, and centralised governance create conditions that cannot be assumed across Europe. What works efficiently in Estonia does not automatically translate to federal states, large economies, or sectors with deeply entrenched legacy systems.

There is also a risk that the “digital exemplar” narrative oversimplifies the complexity of identity at scale. Baltic success stories can obscure the effort required to sustain trust as systems grow and diversify.

The Baltic case underscores an important lesson for EUDI: innovation at small scale is invaluable for learning, but it does not eliminate the need for robust governance, assurance diversity, and operational resilience at European scale.

2.2 The Role of EU-Level Pilot Programs

To support the development of a common European Digital Identity framework, the European Commission has funded a series of Large-Scale Pilots (LSPs). These initiatives bring together Member States, public authorities, and private-sector participants to test specific use cases under real-world conditions.

Key programmes include POTENTIAL, DC4EU, NOBID, EWC, and APTITUDE. While each has a distinct thematic focus — ranging from public services and professional credentials to payments-adjacent and travel-related scenarios — they share a common objective: validating interoperability and trust across borders.

Collectively, these pilots are helping to:

- Test wallet reference architectures and interfaces
- Explore credential issuance and verification flows
- Validate cross-border recognition mechanisms
- Identify gaps in governance and liability models

What they are not designed to do is prove readiness for national or pan-European deployment at population scale. Participation is limited, environments are controlled, and failure modes are constrained. As a result, pilot success should be interpreted as a sign of technical plausibility rather than operational maturity.

2.3 National Participation and Divergent Starting Points

While EU-level pilots provide a shared framework, national participation reflects very different starting conditions. Member States enter the EUDI process with varying degrees of digital identity maturity, institutional complexity, and public trust.

Countries with long-established national eID schemes — such as Germany, the Nordics, and parts of the Benelux — tend to approach pilots as an extension of existing infrastructure. In these contexts, the focus often lies on interoperability, attribute expansion, and private-sector integration.

By contrast, Member States with less mature digital identity ecosystems may view EUDI as an opportunity to leapfrog legacy constraints. For these participants, pilots serve not only as technical experiments but as catalysts for broader institutional reform.

These differences matter. They shape architectural choices, governance expectations, and timelines. They also make uniform rollout scenarios unlikely. Even where technical standards align, organisational and political realities will drive uneven adoption.

2.4 What Pilots Reveal — and What They Hide

The current pilot landscape has already surfaced several important insights. First, wallet-based interactions are technically feasible across borders when supported by agreed standards and trust frameworks. Second, credential exchange can be made user-centric without fundamentally undermining assurance.

At the same time, pilots tend to underexpose the most difficult challenges. Governance arrangements are often simplified. Liability questions are deferred or assumed. Long-term lifecycle management — including revocation, recovery, and update mechanisms — is rarely tested under realistic load.

Pilots also benefit from aligned incentives. Participants are motivated to collaborate, timelines are fixed, and success criteria are predefined. In production environments, these conditions rarely hold. Competing commercial interests, regulatory scrutiny, and public accountability introduce friction that pilots cannot easily simulate.

2.5 The Risk of “Pilot Theatre”

As EUDI pilots multiply, there is a growing risk of what some stakeholders privately describe as “pilot theatre” — a situation in which visible progress masks unresolved structural issues.

This risk does not stem from a lack of effort or expertise. Rather, it reflects the natural tendency of pilot programmes to optimise for demonstration rather than durability. Without a clear pathway from experimentation to operational ownership, pilots can inadvertently delay difficult decisions around funding, governance, and accountability.

Avoiding this outcome will require deliberate transition planning. Pilot results must be translated into production criteria, and responsibilities must shift from project consortia to permanent institutions. This transition, more than any technical milestone, will determine the pace and credibility of EUDI deployment.

2.6 Uneven Progress as a Structural Reality

One of the most consistent signals emerging from the pilot landscape is that progress will be uneven by design. Differences in national governance models, sectoral priorities, and risk tolerance ensure that EUDI will advance at different speeds across Europe.

Rather than viewing this as a failure, it may be more productive to recognise uneven progress as an inherent feature of infrastructure-scale systems. Early adopters will test boundaries and surface failure modes. Others will follow once patterns stabilise.

The challenge for policymakers and market participants alike is to manage this diversity without fragmenting trust. Interoperability frameworks must accommodate variation while preserving a minimum common baseline. Achieving this balance is arguably the central task of the pilot phase.

2.7 From Experiments to Commitments

Ultimately, the value of the current pilot landscape lies not in the number of use cases demonstrated, but in the clarity it provides about what comes next. Moving from pilots to production will require explicit commitments — financial, institutional, and political.

This transition will force questions that pilots can postpone: who operates the infrastructure, who bears liability, how costs are distributed, and how success is measured over time. Until these questions are addressed, EUDI will remain an ambitious framework in search of operational grounding.

The following section turns to one of the most persistent misconceptions revealed by the pilot phase: the assumption that digital wallets themselves are the primary challenge. In practice, they are only the most visible component of a far more complex system.

Sources and References

- European Commission, European Digital Identity Wallet Large-Scale Pilots documentation.
- European Commission, Digital Europe Programme funding calls and project descriptions.
- POTENTIAL Consortium, public project materials and interim reports.
- DC4EU Consortium, public documentation and use-case descriptions.
- NOBID Consortium, programme overview and technical publications.
- ENISA, Interoperability of Digital Identity Systems in the EU.
- European Court of Auditors, reports on large-scale EU digital programmes.

3. Wallets Are Not the Hard Part

Among policymakers, vendors, and even some enterprise stakeholders, discussion of the European Digital Identity Wallet often gravitates toward the wallet itself. User experience, interface design, and feature parity with consumer applications dominate much of the public narrative. This focus is understandable: wallets are tangible, demonstrable, and easy to showcase.

Yet the emphasis on wallets obscures a more fundamental reality. Digital wallets are not the primary challenge facing EUDI. They are the most visible component of a much larger and more complex system. Treating the wallet as the centre of gravity risks underestimating the structural work required to make digital identity function reliably at scale.

3.1 The Visibility Trap

Wallets sit at the intersection between users and identity infrastructure. They are the point of interaction through which credentials are stored, presented, and managed. As such, they naturally attract attention during pilot demonstrations and public communications.

However, visibility should not be confused with importance. A well-designed wallet can mask significant fragility beneath the surface. In pilot environments, where participation is limited and trust assumptions are aligned, this fragility may remain hidden. At scale, it becomes impossible to ignore.

Focusing too heavily on wallet features risks creating a false sense of progress. It suggests that identity deployment is primarily a product challenge, when in reality it is an infrastructure challenge involving governance, assurance, and long-term operational responsibility.

3.2 The Hidden Layers of Digital Identity

Behind every wallet interaction lies a stack of systems and relationships that determine whether trust can be established and sustained. These layers include credential issuers, attribute providers, verification services, trust registries, and governance authorities.

Each layer introduces its own complexity. Issuers must meet assurance requirements and maintain accurate records over time. Verifiers must be able to

assess the validity and relevance of credentials in context. Trust frameworks must define roles, responsibilities, and acceptable risk thresholds across borders.

At pilot scale, these relationships are often simplified or manually coordinated. In production environments, they must operate autonomously and reliably, often under regulatory scrutiny. Failure at any layer undermines confidence in the system as a whole, regardless of wallet quality.

3.3 Lifecycle Management at Scale

One of the least visible challenges in digital identity deployment is lifecycle management. Credentials are not static artefacts. They must be issued, updated, suspended, revoked, and in some cases recovered. Each of these actions carries operational and legal implications.

At population scale, lifecycle events occur continuously and unpredictably. Lost devices, expired credentials, organisational changes, and compromised keys are routine occurrences. Systems must be designed to handle these events without introducing friction that discourages adoption or creates security gaps.

Pilot programmes rarely stress-test lifecycle management under realistic conditions. As a result, the transition to production often exposes weaknesses that were not apparent during experimentation. Addressing these weaknesses requires investment in processes and governance, not just technology.

3.4 Governance, Liability, and Trust

Trust in digital identity systems is not generated by cryptography alone. It is underpinned by clear governance arrangements and credible liability models. When identity assertions fail, stakeholders must know who is responsible and how remediation occurs.

In the context of EUDI, governance questions extend across national and sectoral boundaries. Who accredits issuers and verifiers? How are disputes resolved across jurisdictions? What happens when a credential issued in one country causes harm in another?

These questions are often acknowledged but deferred during pilot phases. In production environments, they become unavoidable. Without clear answers, organisations may hesitate to rely on EUDI credentials for high-value or high-risk transactions, regardless of wallet availability.

3.5 The Limits of Wallet-Centric Thinking

Assuming that widespread wallet deployment will automatically produce a functioning identity ecosystem overlooks the selective nature of trust. Different sectors have different assurance requirements, risk tolerances, and regulatory obligations.

As a result, there is unlikely to be a single wallet configuration suitable for all use cases. Financial services, healthcare, mobility, and employment each impose distinct demands on identity systems. Enterprises will therefore adopt EUDI selectively, integrating wallet-based interactions where they add value and maintaining existing mechanisms elsewhere.

Recognising these limits is not a sign of failure. It reflects the reality of complex digital ecosystems. Designing for selective adoption is more sustainable than pursuing uniformity at the expense of trust.

3.6 Reframing the Challenge

Understanding that wallets are not the hard part allows the EUDI conversation to mature. It shifts attention toward the less visible but more consequential elements of identity infrastructure: governance, interoperability, lifecycle management, and accountability.

This reframing does not diminish the importance of user experience. Rather, it situates usability within a broader system that must earn trust over time. A wallet that is easy to use but poorly governed will not succeed at scale.

The next section examines how these underlying challenges intensify when digital identity systems move beyond pilot environments and into population- and enterprise-scale deployment.

Sources and References

- ENISA, Threat Landscape for Identity and Access Management.
- ISO/IEC 24760, A framework for identity management.
- European Commission, Architecture and Reference Framework for the European Digital Identity Wallet.
- NIST, Digital Identity Guidelines (SP 800-63).
- OECD, Digital Security Risk Management for Economic and Social Prosperity.

4. Identity at Scale: The Real Challenges

Moving digital identity from pilot environments into sustained, large-scale operation introduces a set of challenges that differ fundamentally in nature from those encountered during experimentation. At scale, identity systems must operate continuously, withstand failure, and support diverse use cases without compromising trust. These requirements expose structural pressures that are easy to underestimate when focus remains on individual components such as wallets or credentials.

4.1 Interoperability Beyond Standards

Interoperability is often framed as a standards problem. While common technical standards are a necessary foundation, they are not sufficient on their own. At scale, interoperability is as much organisational and procedural as it is technical.

Different sectors interpret assurance levels, risk thresholds, and compliance obligations in different ways. Even when credentials conform to shared specifications, their acceptance depends on contextual trust decisions made by verifiers. These decisions are shaped by regulation, liability exposure, and business risk rather than by technical compatibility alone.

Cross-border interoperability compounds these challenges. Legal interpretations, supervisory practices, and enforcement cultures vary across Member States. As a result, identity systems must accommodate divergence while maintaining a baseline of mutual trust. Achieving this balance requires governance mechanisms that extend beyond protocol alignment.

4.2 Scale Exposes Operational Reality

At population scale, identity systems become operational infrastructure. Availability, incident response, and continuity planning take precedence over feature development. Downtime, even if rare, has systemic consequences when identity underpins access to essential services.

Scale also amplifies edge cases. Scenarios that occur infrequently in pilots—such as mass credential revocation, coordinated fraud attempts, or systemic component failure—become statistically inevitable. Systems must therefore be

designed not only to function under ideal conditions, but to degrade gracefully under stress.

Operational maturity is rarely visible during pilot phases. It emerges only through sustained operation, real-world incidents, and iterative governance adjustments. This reality reinforces the need to treat EUDI as long-term infrastructure rather than as a deployment milestone.

4.3 Hardware and Software Roots of Trust

Trust at scale depends on anchoring digital identity to credible roots of trust. Software-based mechanisms offer flexibility and rapid iteration, but they also introduce exposure to compromise, cloning, and large-scale attack.

Hardware-backed security elements—such as secure elements, trusted execution environments, and tamper-resistant components—provide stronger assurances for key storage and credential protection. Their use is already well established in domains such as payments and government identity documents.

In the context of EUDI, decisions around hardware versus software roots of trust will influence cost, usability, and risk profiles. There is unlikely to be a single optimal approach. Instead, different assurance levels and use cases will justify different trust anchors. Designing for this diversity is essential to avoid forcing low-risk and high-risk interactions into the same security model.

4.4 Longevity and Cryptographic Agility

Identity infrastructure is expected to endure for decades. This longevity introduces a requirement for cryptographic agility: the ability to adapt security mechanisms over time without wholesale system replacement.

Emerging concerns around quantum computing reinforce this need. While large-scale quantum attacks are not an immediate operational threat, identity credentials issued today may need to remain valid well into a post-quantum future. Planning for algorithm transitions and credential renewal cycles is therefore a strategic consideration rather than a theoretical one.

At scale, cryptographic transitions are complex and resource-intensive. Systems that do not anticipate change risk accumulating technical debt that undermines long-term trust. Incorporating agility into EUDI architectures is a prerequisite for sustainability.

4.5 Governance at Population and Enterprise Scale

As identity systems expand, governance structures must scale alongside them. Informal coordination and project-based oversight are insufficient once identity becomes embedded in daily economic and social activity.

Effective governance requires clear allocation of roles, transparent decision-making processes, and mechanisms for dispute resolution. It must also reconcile public-sector accountability with private-sector participation, particularly where enterprises rely on EUDI credentials for regulated activities.

Failure to establish scalable governance frameworks risks fragmenting trust. Different sectors may develop parallel acceptance criteria, undermining the promise of interoperability. Addressing this risk requires early and sustained attention to governance design, not as an afterthought but as a core component of infrastructure planning.

4.6 Accepting Complexity Without Paralysis

The challenges outlined above underscore a central tension in digital identity deployment at scale. Complexity is unavoidable, but it must not become paralysing. Over-simplification erodes trust, while over-engineering delays adoption.

Successful infrastructure systems balance these pressures by defining minimum viable trust baselines and allowing controlled variation above them. For EUDI, this means establishing common foundations while enabling sector-specific evolution.

Recognising identity at scale as a complex system rather than a uniform solution allows expectations to be managed realistically. It also provides a framework for incremental progress that aligns with the diverse needs of Europe's digital economy.

The next section turns from systemic challenges to the practical implications for enterprises, examining how organisations are likely to engage with EUDI in real operational contexts.

Sources and References

- ENISA, Threat Landscape for Identity and Access Management.
- European Commission, Architecture and Reference Framework for the European Digital Identity Wallet.
- ETSI, standards on trust services and secure elements.
- NIST, Cryptographic Agility and Lifecycle Management publications.
- OECD, Digital Security Risk Management guidelines.

5. Enterprise Reality Check

For enterprises, the European Digital Identity Wallet represents neither a turnkey solution nor an abstract policy exercise. It arrives as a new variable in already complex identity, security, and compliance environments. While much of the public discussion around EUDI focuses on citizen-facing use cases, its long-term impact will be determined by how organisations choose to engage with it in practice.

This engagement is unlikely to be uniform or immediate. Enterprises will adopt EUDI selectively, guided by risk, regulation, and commercial incentive rather than by regulatory ambition alone.

5.1 EUDI Meets Existing Enterprise Identity Stacks

Most medium and large organisations already operate mature identity and access management (IAM) infrastructures. These systems underpin employee access, partner relationships, customer onboarding, and regulatory compliance. Introducing EUDI credentials into this landscape does not replace existing systems; it adds another trust signal that must be evaluated and integrated.

In practice, enterprises will treat EUDI as an external identity source, similar in principle to bank-issued credentials or trusted third-party attestations. Decisions about acceptance will depend on assurance levels, liability exposure, and alignment with internal risk models.

This reality challenges simplistic narratives that frame EUDI as a universal login mechanism. For enterprises, identity is contextual. A credential that is sufficient for one interaction may be inadequate for another. Integration strategies will therefore prioritise flexibility over uniformity.

5.2 Selective Adoption by Sector

Different sectors face different regulatory and operational pressures, shaping how they are likely to engage with EUDI.

In financial services, strong customer authentication, know-your-customer obligations, and anti-money laundering requirements impose high assurance thresholds. EUDI credentials may streamline parts of onboarding or attribute verification, but they will coexist with sector-specific controls rather than replace them.

In mobility and travel, cross-border interoperability offers clearer immediate value. Here, EUDI has the potential to reduce friction while maintaining trust, particularly where credentials can be reused across jurisdictions.

Employment, education, and professional services present another set of opportunities, especially around qualification and status verification. In these contexts, EUDI's attribute-based model aligns well with existing processes, provided governance and liability questions are resolved.

These examples illustrate a broader pattern: enterprises will adopt EUDI where it reduces cost or complexity without increasing risk. Where those conditions are not met, adoption will lag.

5.3 The Liability Question

One of the most significant barriers to enterprise adoption is uncertainty around liability. When an organisation relies on an external identity credential and that credential proves inaccurate or compromised, responsibility must be clearly defined.

In pilot discussions, liability is often assumed rather than tested. Enterprises, however, operate in environments where accountability is enforced through regulation, contracts, and courts. Without clear frameworks governing issuer responsibility, verifier reliance, and dispute resolution, organisations will limit their exposure.

Resolving these issues is not merely a legal exercise. It shapes technical design, assurance models, and acceptance criteria. Enterprises will look for explicit guidance and precedents before embedding EUDI credentials into high-value workflows.

5.4 Operational Integration and Cost

Beyond trust considerations, practical integration challenges influence adoption decisions. Supporting EUDI interactions requires investment in systems, processes, and staff training. For many organisations, the business case will depend on whether these costs are offset by measurable efficiency gains.

Early adopters are likely to focus on bounded use cases with clear return on investment. These may include reducing manual verification steps, improving cross-border reach, or enhancing user experience in regulated interactions.

Wider deployment will follow only if operational benefits scale and integration complexity stabilises. Enterprises are accustomed to incremental change; few will commit to wholesale transformation based on pilot-phase signals alone.

5.5 Trust, Brand, and User Expectations

Enterprises must also consider the impact of EUDI interactions on user trust and brand perception. While EUDI emphasises user control and data minimisation, implementation choices influence how these principles are experienced in practice.

Poorly integrated identity flows can create confusion or frustration, undermining confidence in both the service provider and the identity system itself. Conversely, well-designed interactions that respect user consent and context can enhance trust.

This places responsibility on enterprises not only to adopt EUDI technically, but to integrate it thoughtfully into customer and employee journeys. Trust is cumulative; early missteps can have lasting consequences.

5.6 Enterprise Readiness Is Uneven

As with national implementations, enterprise readiness varies widely. Large, regulated organisations may have the resources to experiment and integrate selectively. Smaller enterprises may wait for clearer patterns and more mature tooling.

This uneven readiness reinforces the likelihood of phased adoption. EUDI will enter enterprise environments gradually, shaped by sector leaders and regulatory pressure rather than by mass-market momentum.

Understanding this dynamic is essential for realistic planning. Expecting rapid, universal enterprise uptake risks misalignment between policy ambition and market behaviour.

The next section examines how the transition from pilots to production can be managed in light of these realities, and what conditions must be met for EUDI to move beyond experimentation into sustained operation.

Sources and References

- ENISA, Identity and Access Management for Enterprises.
- European Banking Authority (EBA), guidance on customer due diligence and identity verification.
- ISO/IEC 27001 and ISO/IEC 27002 standards on information security management.
- OECD, Trust and Digital Identity.
- European Commission, Impact Assessment accompanying the eIDAS 2.0 proposal.

6. From Pilots to Production

The European Digital Identity Wallet initiative has now reached a decisive inflection point. Pilots have demonstrated feasibility. National approaches have revealed structural diversity. Enterprises have begun to assess where EUDI fits — and where it does not. What remains unresolved is not whether EUDI can work, but how it transitions from controlled experimentation into sustained, accountable operation.

This transition is not automatic. It requires a deliberate shift in mindset, governance, and investment. Without it, EUDI risks remaining a permanent pilot programme: visible, well-funded, and strategically important — yet operationally incomplete.

6.1 The End of Experimentation as a Safe Space

Pilot programmes provide cover. They allow stakeholders to explore architectures, defer liability questions, and operate under exceptional conditions. While this is appropriate in early phases, it becomes a liability once pilots proliferate without a clear path forward.

Moving to production removes this protection. Identity systems must function continuously, support real users at scale, and withstand regulatory and legal scrutiny. Failures can no longer be framed as learning experiences; they become incidents with consequences.

A production mindset therefore demands different criteria for success. Stability, accountability, and resilience replace demonstration and innovation as primary measures. This shift is cultural as much as technical, and it must occur across public authorities, vendors, and relying parties alike.

6.2 Ownership and Operational Responsibility

One of the most significant gaps exposed by the pilot phase is ambiguity around ownership. In pilot environments, responsibility is shared across consortia, funding programmes, and temporary governance structures. In production, this ambiguity is untenable.

Operational identity infrastructure requires clear custodianship. Someone must be responsible for uptime, incident response, compliance, and long-term

maintenance. This applies not only to wallet components, but to trust registries, accreditation mechanisms, and interoperability layers.

Determining ownership is politically sensitive. It touches on national sovereignty, public–private roles, and funding models. Yet without resolution, progress will stall. EUDI cannot scale on goodwill alone.

6.3 Funding Beyond the Pilot Phase

EU-funded pilots lower barriers to entry, but they also mask the true cost of operating identity infrastructure at scale. Production systems require sustained funding for operations, governance, security updates, and support.

This raises unavoidable questions: who pays, and how? Public funding may cover foundational components, but sector-specific deployments often rely on private investment. Aligning incentives across these domains is essential to avoid fragmentation or underinvestment.

Transparent funding models are also a signal of seriousness. Enterprises and service providers are unlikely to integrate EUDI deeply if long-term viability appears uncertain.

6.4 From Reference Architectures to Real Architectures

Reference architectures play an important role in aligning expectations and guiding development. However, production systems are shaped by legacy integration, regulatory interpretation, and operational constraint.

The transition to production will therefore involve divergence from idealised models. This is not a failure of design; it is a feature of real-world deployment. What matters is that divergence remains bounded by agreed trust frameworks and interoperability requirements.

Allowing controlled variation while enforcing common baselines is the defining governance challenge of the next phase.

6.5 Timelines, Expectations, and the Myth of a “Big Bang”

One of the most persistent misconceptions surrounding EUDI is the expectation of a rapid, uniform rollout. The evidence from pilots and national case studies points to a different trajectory.

Production adoption will be incremental. Certain sectors and countries will move earlier, driven by clear use cases or regulatory pressure. Others will follow once patterns stabilise and tooling matures. There will be overlap, coexistence, and periods of uneven progress.

This phased approach is not a weakness. It reflects the realities of infrastructure-scale change. Managing expectations accordingly is essential to maintaining trust in the initiative.

6.6 What Moving to Production Actually Requires

Across the pilot landscape and enterprise engagement, several conditions emerge as prerequisites for transition:

- Clear operational ownership at national and European levels
- Defined liability and reliance frameworks for issuers and verifiers
- Sustainable funding models beyond EU programme cycles
- Governance mechanisms capable of scaling with adoption
- Acceptance of selective and uneven deployment

Absent these conditions, further technical refinement will have limited impact.

6.7 Production as a Trust Commitment

Ultimately, moving from pilots to production is not a technical milestone. It is a trust commitment. It signals that identity systems are reliable enough to underpin economic activity, public services, and regulated interactions over time.

For EUDI, this commitment must be earned gradually, through demonstrated reliability rather than symbolic launches. Success will be measured not by adoption statistics alone, but by the absence of disruption — by identity becoming invisible infrastructure.

The final section of this paper examines what such success looks like in practice, and how Europe might judge progress once pilots are no longer the dominant frame of reference.

Sources and References

- European Commission, Architecture and Reference Framework for the European Digital Identity Wallet
- European Court of Auditors, reports on EU digital programme sustainability
- ENISA, Operational Resilience and Trust Frameworks for Digital Identity
- OECD, Public–Private Collaboration in Digital Infrastructure
- World Bank, Identity Systems and Service Delivery at Scale

7. What Success Looks Like

Success for the European Digital Identity Wallet initiative is often discussed in terms of adoption metrics: the number of wallets issued, credentials stored, or transactions processed. While these indicators have value, they provide an incomplete picture. At infrastructure scale, success is less about visibility and more about reliability, trust, and sustained usefulness.

EUDI's ultimate test will not be how quickly it is deployed, but how well it integrates into Europe's economic and social fabric over time.

7.1 Success Is Gradual and Uneven

A successful EUDI rollout will not occur simultaneously across all Member States or sectors. As the pilot landscape has shown, national starting points, governance models, and risk appetites differ significantly. These differences will continue to shape adoption trajectories.

Some countries and sectors will move earlier, driven by regulatory pressure, clear cross-border needs, or mature identity ecosystems. Others will proceed more cautiously, prioritising legal certainty and institutional alignment. This uneven progress is not a sign of fragmentation; it is a natural outcome of infrastructure-scale change in a diverse political and economic union.

Judging EUDI by uniformity or speed risks misunderstanding its purpose. Progress should instead be assessed by whether early deployments are stable, trusted, and extensible.

7.2 Success Is Largely Invisible to Users

Paradoxically, one of the strongest indicators of success will be a lack of user awareness. When digital identity works well, it recedes into the background. Users focus on the service they are accessing, not on the identity mechanism enabling it.

In successful implementations, EUDI interactions will feel predictable, proportionate, and respectful of context. Identity will not be repeatedly asserted or verified without reason. Consent will be meaningful rather than performative.

This invisibility is particularly important in enterprise and regulated environments, where friction erodes trust and operational efficiency. Identity that demands attention has failed its primary function.

7.3 Success Preserves Trust Without Overreach

EUDI aims to strengthen trust while enhancing user control. Achieving this balance requires restraint as well as capability. Not every interaction requires the highest possible assurance level, and not every credential needs to be universally reusable.

Successful EUDI deployments will apply assurance proportionately, aligning verification strength with risk. Overuse of high-assurance identity in low-risk contexts would undermine user confidence and discourage adoption.

Trust is preserved when identity systems are predictable, transparent, and limited in scope. Success therefore depends as much on what EUDI chooses not to do as on what it enables.

7.4 Success Enables Selective Enterprise Adoption

For enterprises, success will not be defined by wholesale replacement of existing identity systems. Instead, EUDI will succeed when it integrates cleanly into established IAM, compliance, and onboarding processes.

Enterprises will adopt EUDI where it reduces duplication, improves assurance, or supports cross-border interaction. In other areas, existing mechanisms will remain in place. This coexistence is a feature, not a failure.

A successful EUDI ecosystem will support this selectivity without penalising organisations that move at different speeds. Interoperability frameworks must accommodate partial participation while maintaining trust.

7.5 Success Is Measured Over Years, Not Pilots

Perhaps the most important measure of success is longevity. Digital identity infrastructure must remain viable across regulatory cycles, technology shifts, and evolving threat landscapes.

Successful EUDI systems will demonstrate the ability to adapt: to incorporate new credential types, adjust governance models, and evolve cryptographic foundations

without disrupting service continuity. This adaptability is a stronger indicator of maturity than early adoption figures.

In this sense, EUDI success will be most evident after pilots have faded from view — when identity systems are no longer the subject of projects, but a stable part of digital operations.

7.6 Europe's Broader Influence

If EUDI succeeds on these terms, its influence will extend beyond Europe. A functioning, federated, rights-respecting digital identity framework at continental scale would represent a meaningful alternative to platform-centric identity models.

This influence will not come from export or enforcement, but from demonstration. Showing that digital identity can operate as public infrastructure — interoperable, governed, and trusted — may prove to be Europe's most significant contribution to the global identity debate.

Success, in this context, is not a destination but a condition: identity that works quietly, reliably, and at scale.

Sources and References

- European Commission, eIDAS 2.0 Impact Assessments and Policy Briefings
- ENISA, Digital Identity Trust Models
- OECD, Building Trust in Digital Government
- World Economic Forum, Digital Identity: On the Threshold of a Digital Identity Revolution
- European Data Protection Supervisor (EDPS), opinions on digital identity and proportionality

Closing Summary

The European Digital Identity Wallet initiative has moved decisively beyond theory. The question facing Europe is no longer whether digital identity wallets can function across borders, but whether identity can be operated as durable, trusted infrastructure at continental scale.

This paper has shown that pilots have served their purpose. They have demonstrated feasibility, surfaced architectural patterns, and revealed the diversity of national starting points. What they have not — and cannot — resolve on their own are the structural challenges that define production systems: governance, liability, operational ownership, and long-term sustainability.

Evidence from national implementations makes one conclusion unavoidable: EUDI will not arrive uniformly. Germany's assurance-first approach, the Nordics' trust-driven acceleration, the Netherlands' pragmatic service integration, and the Baltics' digital-first agility each reflect legitimate responses to local conditions. Together, they confirm that variation is not a temporary deviation, but a permanent feature of Europe's identity landscape.

For enterprises, this reality demands realism. EUDI will not replace existing identity systems wholesale, nor will it eliminate sector-specific controls. Its value lies in selective integration — where wallet-based credentials reduce friction, improve assurance, or enable cross-border interaction without increasing risk. Clear liability frameworks and operational predictability will ultimately determine adoption.

The transition from pilots to production is therefore a governance challenge as much as a technical one. Progress now depends on explicit commitments: who operates the infrastructure, how trust is maintained, how costs are sustained, and how accountability is enforced over time. Without these decisions, further technical refinement will yield diminishing returns.

Success for EUDI should be judged cautiously and over time. At scale, identity infrastructure succeeds when it becomes largely invisible — reliable, proportionate, and embedded in everyday digital interactions. Rapid uptake and headline metrics matter less than stability, trust, and adaptability.

If Europe succeeds on these terms, it will have achieved something rare: a federated digital identity framework that balances interoperability with

sovereignty, innovation with restraint, and user control with institutional trust. That outcome would not only strengthen Europe's digital economy, but also demonstrate that digital identity can function as public infrastructure — quietly, credibly, and at scale.

Appendix A: Country Pilot Profiles (Condensed Reference Edition)

This appendix provides structured national snapshots of selected European Digital Identity (EUDI) pilot engagements. It is intended as a reference section to support the analysis presented in the main paper, offering factual grounding without ranking or comparative scoring.

Germany

Governance
Federal Ministry of the Interior and Community (BMI), Federal Office for Information Security (BSI), Länder authorities. Strong federal structure with high legal and security thresholds.

EUDI Engagement
Participation in multiple EU Large-Scale Pilots covering public administration, professional credentials, and regulated access.

Wallet Model
Federally coordinated framework with delegated and sector-specific implementations. Wallet treated as an interface layered onto existing national trust anchors.

Credential Scope
Identity attributes, professional qualifications, regulated access credentials.

Private Sector
Active involvement of certified technology and trust service providers.

Stage
Advanced pilot phase; production transition constrained by coordination and funding complexity.

Key Strength
High assurance and legal robustness.

Key Challenge
Federal–Länder coordination and operational ownership at scale.

Nordics (Norway, Finland, Sweden – NOBID)

Governance
Centralised digital authorities with deep public–private collaboration, particularly involving financial institutions.

EUDI Engagement
Nordic-Baltic EUDI Large-Scale Pilot (NOBID), focused on cross-border reuse and payments-adjacent identity.

Wallet Model
Pluralistic wallet ecosystem aligned to shared trust frameworks rather than a single state wallet.

Credential Scope
Identity, financial, service-access, and professional attributes.

Private Sector
Strong role for banks and private identity providers.

Stage
Mature pilots with selective production readiness.

Key Strength
High public trust and strong market pull.

Key Challenge
Limited transferability to larger, more fragmented Member States.

Netherlands

Governance
Centrally coordinated with strong service orientation and clear role separation between public and private actors.

EUDI Engagement
Participation in multiple pilots focused on public services, business access, and attribute-based verification.

Wallet Model
Wallets treated as modular service components, integrated into existing digital journeys.

Credential Scope
Identity attributes, professional and organisational credentials.

Private Sector
Active involvement of service providers and integrators.

Stage
Well-scoped pilots with realistic paths to production.

Key Strength
Operational pragmatism and predictability.

Key Challenge
Scaling service-centric models to broader cross-border complexity.

Baltics (Estonia, Latvia, Lithuania)

Governance
Centralised digital agencies with strong political backing and high digital literacy.

EUDI Engagement
Focus on interoperability and extension of existing national digital identity systems.

Wallet Model
Predominantly software-centric architectures supported by institutional trust.

Credential Scope
Identity attributes, public service, and business credentials.

Private Sector
Moderate participation, aligned closely with government-led services.

Stage
Functionally mature pilots within domestic contexts.

Key Strength
Speed and clarity of implementation.

Key Challenge
Scalability and applicability to larger, more complex environments.

France

Governance
Strongly centralised, state-led identity governance involving the Ministry of the Interior, DINUM, and ANSSI.

EUDI Engagement
Participation in EU pilots with emphasis on public-sector identity and sovereign alignment.

Wallet Model
State-centric wallet closely integrated with national digital identity platforms.

Credential Scope
Identity attributes, public service access, selected entitlement credentials.

Private Sector
Limited; primarily technology providers rather than issuers.

Stage
Advanced public-sector pilots; cautious extension to private-sector use cases.

Key Strength
Clear accountability and sovereign control.

Key Challenge
Flexibility and integration with market-driven identity ecosystems.

Italy

Governance
Hybrid model combining central coordination (AgID, Ministry of the Interior) with accredited private identity providers.

EUDI Engagement
Pilots focused on interoperability with existing national digital identity systems.

Wallet Model
Delegated wallet ecosystem under national accreditation schemes.

Credential Scope
Identity attributes, public service, organisational and professional credentials.

Private Sector
Significant role for accredited providers.

Stage
Mature national identity deployment; EUDI focused on extension rather than replacement.

Key Strength
Scalable public–private delegation model.

Key Challenge
Consistency across regions and providers.

Spain

Governance
Central coordination with significant regional autonomy.

EUDI Engagement
Pilot participation centred on public administration and cross-border services.

Wallet Model
Public-sector-led wallet integrated with government digital services.

Credential Scope
Identity attributes, public service access, selected professional credentials.

Private Sector
Limited but growing involvement.

Stage
Active pilot phase with gradual progression.

Key Strength
Strong public-sector digitalisation agenda.

Key Challenge
Regional coordination and slower enterprise uptake.

Interpretive Note
These profiles demonstrate that EUDI implementation is shaped primarily by national governance models rather than technical capability. Centralised, delegated, and hybrid approaches can all function within the EUDI framework, but each carries distinct trade-offs in speed, assurance, flexibility, and market engagement.

Table 1: Governance & Structural Model

Country	**Governance Model**	**Degree of Centralisation**	**Public–Private Model**	**Institutional Complexity**
Germany	Federal	Low	Regulated, certification-heavy	High
Nordics	Centralised	High	Strong bank-led cooperation	Low
Netherlands	Central coordination	Medium	Service-oriented partnership	Medium
Baltics	Centralised	High	Government-led	Low
France	State-centric	Very high	Limited private issuance	Medium
Italy	Hybrid	Medium	Delegated accredited providers	Medium–High
Spain	Hybrid	Medium	Public-sector led	High (regional)

Note: Governance structures strongly influence rollout speed and operational complexity.

Table 2: Wallet & Trust Architecture

Country	Wallet Model	Trust Anchor Bias	Assurance Philosophy	Interoperability Stance
Germany	Federated / delegated	Hardware-rooted	High assurance first	Rules-driven
Nordics (NOBID)	Pluralistic	Software + institutional trust	Risk-proportionate	Market-driven
Netherlands	Modular service wallet	Balanced	Use-case driven	Pragmatic
Baltics	Software-centric	Institutional trust	Practical sufficiency	Extension-focused
France	State wallet	State-backed	Sovereign assurance	Controlled
Italy	Delegated wallets	Mixed	Accreditation-based	Structured
Spain	Public wallet	State-backed	Compliance-first	Gradual

Note: There is no single "EUDI wallet model"; national trust assumptions dominate.

Table 3: Enterprise & Market Readiness

Country	Enterprise Readiness	Likely Early Sectors	Adoption Pattern	Key Enterprise Constraint
Germany	Medium	Regulated industry, manufacturing	Gradual, assurance-led	Complexity and liability
Nordics (NOBID)	High	Finance, services, mobility	Fast, selective	Limited scalability
Netherlands	Medium–High	GovTech, regulated services	Incremental	Cross-border scope
Baltics	Medium	Public services, SMEs	Fast domestically	Market size
France	Medium	Public services	State-led	Private-sector pull
Italy	Medium	Public and regulated services	Delegated growth	Consistency across providers
Spain	Medium–Low	Public administration	Slow expansion	Regional fragmentation

Note: Enterprise adoption is expected to be selective and sector-specific.

Appendix B: Terminology and Definitions

This appendix provides concise definitions of key terms used throughout this whitepaper. The aim is to ensure clarity and consistency for policymakers, enterprise decision-makers, and technology providers, and to reduce ambiguity when interpreting the European Digital Identity (EUDI) framework.

The definitions reflect common usage across EU policy, standards bodies, and industry practice. They are descriptive rather than normative.

European Digital Identity (EUDI)

A European Union initiative established under the revised electronic Identification, Authentication and Trust Services Regulation (eIDAS 2.0), intended to provide a harmonised framework for digital identity and attribute verification across Member States while preserving national sovereignty over identity issuance.

European Digital Identity Wallet (EUDI Wallet)

A digital application or service that allows individuals or organisations to store, manage, and present identity credentials and verified attributes issued by trusted sources. The wallet acts as an interaction layer between holders, issuers, and verifiers within the EUDI framework.

Credential / Verifiable Credential

A digitally signed statement issued by a trusted authority that attests to one or more attributes of an individual or organisation (e.g. identity, qualification, entitlement). Verifiable credentials can be cryptographically checked by a verifier without direct interaction with the issuer.

Issuer

An entity authorised within a trust framework to issue credentials. Issuers may include public authorities, regulated private organisations, or accredited service providers, depending on national implementation models.

Holder

The individual or organisation to whom a credential is issued and who controls its storage and presentation, typically via a digital wallet.

Verifier / Relying Party

An entity that requests and verifies credentials in order to grant access to a service, confirm an attribute, or complete a transaction. Verifiers make contextual trust decisions based on assurance level, risk, and regulatory requirements.

Trust Framework

A set of rules, policies, technical standards, and governance mechanisms that define how issuers, holders, and verifiers interact, including eligibility, accreditation, assurance levels, and liability arrangements.

Assurance Level

A measure of confidence in the validity of an identity or credential, based on factors such as identity proofing, authentication strength, and credential protection. Assurance levels are applied proportionately according to use-case risk.

Identity and Access Management (IAM)

Enterprise systems and processes used to manage digital identities, control access to resources, and enforce authentication and authorisation policies for employees, partners, and customers.

Attribute-Based Identity

An identity model in which specific attributes (e.g. age, qualification, residency) are presented independently of a full identity profile, supporting data minimisation and contextual disclosure.

Root of Trust

The foundational element on which trust in a digital identity system is built. Roots of trust may be software-based (e.g. cryptographic keys protected by operating systems) or hardware-based (e.g. secure elements or trusted execution environments).

Hardware Root of Trust

A security mechanism implemented in tamper-resistant hardware that provides strong protection for cryptographic keys and identity credentials. Common in national ID documents, payment systems, and high-assurance environments.

Software Root of Trust

A trust mechanism implemented primarily in software, relying on operating system security, cryptography, and institutional controls rather than dedicated hardware components.

Lifecycle Management

The processes governing the creation, update, suspension, revocation, and expiration of identity credentials over time. Effective lifecycle management is critical for maintaining trust at scale.

Interoperability

The ability of different identity systems, wallets, and services to work together across organisational, sectoral, and national boundaries while maintaining agreed trust and assurance levels.

Selective Adoption

An enterprise adoption pattern in which new identity mechanisms are integrated only where they add clear value or reduce risk, rather than replacing existing systems wholesale.

Pilot Programme / Large-Scale Pilot (LSP)

An EU-funded initiative designed to test technical, organisational, and governance aspects of EUDI implementation under controlled conditions. Pilots are exploratory by design and do not represent production readiness.

Production Deployment

The sustained, operational use of identity systems at population or enterprise scale, characterized by defined ownership, liability, funding, and governance structures.

Identity as Infrastructure

A conceptual framing that treats digital identity as foundational, long-lived public infrastructure rather than as a discrete application or product. Emphasises reliability, governance, and long-term trust over novelty.

Note on Usage

These definitions are intended to support understanding of this whitepaper and should not be interpreted as legal definitions unless explicitly stated in regulation or implementing acts.

Appendix C: References and Further Reading

This appendix consolidates key regulatory texts, policy documents, standards, and analytical resources relevant to the European Digital Identity (EUDI) framework. It is intended to support further investigation and provide source material underpinning the analysis presented in this whitepaper.

The references are grouped by category for ease of use.

EU Regulation and Policy

- European Commission, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
- European Commission, Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (eIDAS 2.0).
- European Commission, Impact Assessment accompanying the proposal for a European Digital Identity Framework.
- European Commission, 2030 Digital Compass: the European Way for the Digital Decade.
- Council of the European Union, General Approach on the European Digital Identity Regulation.
- European Parliament, Committee reports and amendments related to eIDAS 2.0.

EUDI Architecture and Pilot Programs

- European Commission, Architecture and Reference Framework (ARF) for the European Digital Identity Wallet.
- European Commission, European Digital Identity Wallet Large-Scale Pilots (LSPs) programme documentation.
- POTENTIAL Consortium, Public deliverables and technical reports.
- DC4EU Consortium, Use-case descriptions and interim findings.
- NOBID Consortium, Nordic–Baltic EUDI pilot documentation.
- EWC and APTITUDE Consortia, Public project materials and outcomes.

Cybersecurity, Trust, and Risk

- European Union Agency for Cybersecurity (ENISA), Threat Landscape for Identity and Access Management.
- ENISA, Trust Services and Digital Identity in the EU.
- ENISA, Interoperability of Digital Identity Systems.
- European Data Protection Board (EDPB), Opinions and guidance on digital identity and attribute sharing.
- European Data Protection Supervisor (EDPS), Opinions on digital identity, proportionality, and user control.

Standards and Technical References

- ISO/IEC 24760, A Framework for Identity Management.
- ISO/IEC 27001 and ISO/IEC 27002, Information Security Management Systems.
- ETSI standards on trust services, electronic signatures, and secure elements.
- NIST SP 800-63, Digital Identity Guidelines.
- W3C, Verifiable Credentials Data Model.

Enterprise, Economic, and Governance Perspectives

- Organisation for Economic Co-operation and Development (OECD), Digital Security Risk Management for Economic and Social Prosperity.
- OECD, Building Trust in Digital Government.
- World Bank, Identity Systems and Service Delivery at Scale.
- World Economic Forum, Digital Identity: On the Threshold of a Digital Identity Revolution.
- European Court of Auditors, Reports on the sustainability and governance of EU digital programmes.

Post-Quantum and Long-Term Security Context

- European Commission, EU Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.
- ENISA, Post-Quantum Cryptography: Current State and Quantum Readiness.
- National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Standardisation Project.

Note on Sources

This whitepaper draws on publicly available documentation, standards, and expert analysis. References are provided for informational purposes and do not imply endorsement of specific technologies, vendors, or implementation models.

About The Quantum Space

The Quantum Space (TQS) is an independent research and intelligence platform dedicated to quantum computing, post-quantum cryptography, cybersecurity, and digital sovereignty. Our mission is to equip Europe's decision-makers with actionable, evidence-based insights to anticipate and adapt to the quantum era.

We specialise in sector-specific strategic analysis that bridges the gap between technical depth and boardroom priorities — supporting leaders in technology, defence, finance, and infrastructure with intelligence that is:

- **Technically rigorous** — grounded in verifiable data, technical standards, and leading-edge research.
- **Strategically relevant** — framed in the context of sovereignty, resilience, and competitive advantage.
- **Forward-looking** — identifying not just immediate threats, but the emerging opportunities of quantum technologies.

Our research methodology integrates:

- **Primary source analysis** — EU directives, national strategies, and industry technical publications.
- **Sector engagement** — consultation with vendors, regulators, and operators across critical industries.
- **Comparative intelligence** — mapping Europe's positioning against global competitors in quantum readiness.

TQS operates as an independent voice, committed to transparency and neutrality in its assessments. We work with public-sector agencies seeking to set resilient quantum migration policies and private-sector leaders integrating quantum-safe technologies into mission-critical systems. We also work with industry consortia shaping international standards and collaborative innovation.

https://thequantumspace.org