What we learnt from Europe's biggest Digital Identity experiment.

EUDI Large Scale Pilots, Insights & Recommendations

Meeco Report
January 2026

Contents

Acknowledgements

EWC Consortium: To read more about the EWC Consortium including the final report visit: **https://eudiwalletconsortium.org/**

POTENTIAL Consortium: To read more about the POTENTIAL Consortium including the final report visit: https://digital-identity-wallet.eu

NOBID Consortium: To read more about the NOBID Consortium including technical reports visit: https://www.nobidconsortium.com/NOBID

DC4EU Consortium: To read more about the DC4EU Consortium including technical reports visit: https://dc4eu.eu

Foreword

We stand at a remarkable inflection point in digital identity. What you're about to read represents the largest coordinated digital identity experiment ever conducted: a €46 million undertaking that brought together over 550 organisations across 27 countries to answer a deceptively simple question: *can we build a digital identity system that actually works for people?*

The four Large-Scale Pilots documented in this report, **EWC**, **POTENTIAL**, **NOBID**, and **DC4EU**, represent something unprecedented. Not just in scale, but in ambition. Each consortium brought unique expertise: EWC's focus on travel and payments, POTENTIAL's comprehensive validation across six use cases, NOBID's Nordic-Baltic cross-border innovations, and DC4EU's pioneering work in education and social security.

Together, they tested the European Digital Identity Wallet in over 1,300 interoperability scenarios, issued more than 1,500 credentials, and engaged hundreds of real users in production-ready transactions.

I want to acknowledge the extraordinary effort behind these numbers. The researchers, developers, policy makers, and institutional leaders who participated in these pilots navigated constantly evolving standards, aligned disparate national frameworks, and persevered through the inherent complexity of building something genuinely new.

This wasn't a theoretical exercise, these teams put working wallets in people's hands, processed real transactions, and uncovered the truth about what digital identity demands in practice, not just in principle.

The findings are both encouraging and sobering. The technology works. Cross-border interoperability is achievable. Privacy-by-Design can be operationalised. Yet technical capability alone won't drive adoption. As the EWC consortium discovered, only 29% of citizens would adopt the wallet today. ***The gap isn't technical, it's experiential.*** People need to see clear, tangible value that existing solutions don't provide.

This is where the real work begins. Moving from successful pilots to thriving ecosystems requires more than standards and specifications. It requires infrastructure that makes identity solutions genuinely easy to build, deploy, and integrate.

At Meeco, we've developed the Secure Value Exchange (SVX) Platform precisely for this transition phase, providing the orchestration layer that connects wallets, credentials, and services into coherent experiences that people want to use. ***Because ultimately, adoption happens when technology disappears into seamless, trustworthy interactions***.

The pilots have proven what's possible. Now we must prove what's practical.

I invite you to engage with these findings not as endpoints, but as foundations. The Member States facing imminent deployment deadlines, the enterprises seeking to integrate digital identity, the technology providers building the next generation of solutions. We all have essential roles in translating these learnings into lived reality.

The question isn't whether Europe can build a digital identity ecosystem. These pilots prove it can. The question is whether we can build one that citizens choose to embrace.

That requires us all to think beyond compliance and toward transformation. The journey from pilot to production is just beginning.

Together, let's make it count.

Katryna Dow
CEO & Founder, Meeco
Brussels, January 2026

Europe's Biggest Digital Identity Experiment

Executive summary

Between 2023 and 2025, four major European consortia successfully completed extensive testing of the European Digital Identity Wallet (EUDI Wallet) across diverse real-world scenarios, marking a critical milestone in Europe's digital transformation journey.

The EWC, POTENTIAL, NOBID, and DC4EU pilot programs brought together over 550 organisations from 26 EU member states plus Norway, Iceland, and Ukraine, supported by more than €46 million in EU funding. Together, these initiatives validated the wallet's functionality across 11 distinct use cases spanning travel, payments, education, healthcare, and social security, providing essential evidence for the regulatory framework that will require Member States to deliver EUDI Wallets to citizens by November 2026.

The technical achievements were substantial – working seamlessly when proper standards are implemented

The technical achievements were substantial. Cross-border interoperability testing proved that wallets could function seamlessly across member states when proper standards are implemented.

EWC Consortium
The EWC consortium demonstrated production-ready transactions in travel scenarios, with real ferry tickets purchased using integrated payments, automated airline check-ins, and streamlined hotel registrations.

POTENTIAL
POTENTIAL conducted over 1,300 interoperability tests and 1,000 successful transactions, including 249 cross-border scenarios, validating wallet use for government services, bank account opening, mobile SIM registration, mobile driving licenses, qualified electronic signatures, and electronic prescriptions.

NOBID
NOBID successfully piloted domestic and cross-border payment authorization, digital signatures, and credential sharing across six countries.

DC4EU
DC4EU issued over 1,500 digital educational credentials and pioneered the digitization of Portable Document A1 and European Health Insurance Cards for cross-border use.

Data Protection

Privacy-by-Design principles worked as intended throughout all pilots. Users maintained granular control over their data through selective disclosure mechanisms, sharing only the minimum necessary information for each transaction.

Mobile driving licenses were successfully tested in multiple countries, demonstrating both proximity and remote verification capabilities. The pilots validated that age verification could occur without revealing birth dates, that banking credentials could be issued and verified without excessive data collection, and that health credentials could enable cross-border pharmacy services while protecting sensitive medical information.

Challenges Ahead

However, the pilots also revealed significant challenges that must be addressed before widespread adoption can succeed. Payment integration emerged as substantially more complex than anticipated, requiring careful alignment with existing payment infrastructure and PSD2 compliance frameworks.

Only 29% of EU citizens would adopt the wallet in its current form

User adoption research conducted by EWC revealed that only 29% of EU citizens would adopt the wallet in its current form, primarily because existing digital solutions work "well enough" for most people and security concerns outweigh perceived benefits for many users. The fundamental question citizens ask is "what's in it for me?" rather than "what's good for the EU?" This gap between technical capability and user motivation represents the most critical barrier to adoption.

Standards Alignment

Standards alignment proved crucial yet challenging. The pilots identified significant differences in how member states adopted specifications, with fragmented certification approaches and varied implementations of the Architecture Reference Framework (ARF).

The constant evolution of technical standards disrupted development across all consortia, with frequent updates to ARF, Reference Implementation, and OpenID4VC specifications causing version mismatches between partners. Semantic interoperability gaps emerged as a persistent challenge, with no common data models for addresses, diplomas, educational credentials, or citizen data across member states. These technical fragmentation issues risk undermining the entire ecosystem if not resolved through mandatory EU-wide standards and conformance testing.

Governance & Business Models

Governance structures emerged as a determining factor in pilot success. Member states with dedicated coordination bodies and strong inter-ministerial collaboration advanced faster and encountered fewer obstacles.

Member states with dedicated coordination bodies and strong inter-ministerial collaboration advanced faster

The pilots demonstrated that public-private partnerships are not optional but essential, requiring banks, telecommunications operators, trust service providers, and technology companies to be involved from the outset.

However, sustainable business models remain unclear for all stakeholders. Questions of who pays for wallet operations, credential issuance, verification services, and authentication when end users access services for free have not been satisfactorily answered. Without viable commercial models, even technically successful solutions may fail to achieve market adoption.

Regulation

Legal and regulatory frameworks lag technical readiness. Anti-money laundering regulations do not explicitly recognise wallet attestations, creating uncertainty for financial institutions attempting to integrate wallet-based KYC/AML processes.

Liability frameworks remain unclear, with banks and other relying parties lacking certainty about responsibility when depending on wallet credentials. Regulatory recognition varies significantly across member states and sectors, with some telecom operators and healthcare providers requiring additional legal clarity before committing to production deployment.

The absence of harmonised legal frameworks for representation, including parental authority, guardianship, and business mandates, creates particular challenges for cross-border scenarios.

User Experience

User experience design emerged as equally important as technical security. Pilots revealed confusing multi-step flows, unclear data sharing requests, language barriers, and significant accessibility issues for persons with disabilities. Citizens expressed concern about complex onboarding processes and inconsistent user interfaces across member states.

The pilots confirmed that privacy and transparency matter as much as regulatory compliance. Wallet adoption will fail without privacy-by-design principles, clear communication about data usage, and consistent design standards that meet or exceed current digital service benchmarks rather than merely matching them.

Implementation Roadmap

Looking ahead to the mandatory 2026 deployment deadline, member states face substantial implementation challenges. Public services must be configured to accept wallets, meeting "High" levels of assurance requirements while ensuring accessibility and usability.

Private sector acceptance, mandated for banking and regulated industries by December 2027, requires extensive integration with existing infrastructure, robust security certification frameworks, and clear business incentives.

Two new pilot programs launched in 2025, APTITUDE and WE BUILD, will continue testing business wallets and advanced use cases, building on the foundation established by the initial four consortia.

Mandated acceptance, for regulated industries by December 2027, requires extensive integration with existing infrastructure, robust security certification frameworks, and clear business incentives.

The path forward requires coordinated action across multiple dimensions. Member states must accelerate alignment with the Architecture Reference Framework and implementing acts under eIDAS 2.0, establishing strong national governance structures complemented by EU-level coordination forums.

Mandatory interoperability testing through European-level conformance environments must be instituted before market entry. User-centric design must be prioritized, with EU-level UX guidelines ensuring consistency and accessibility across implementations.

Trust-building communication campaigns must explain wallet benefits in everyday scenarios rather than abstract policy terms. Private sector integration must occur from the outset, particularly in banking, telecommunications, and healthcare, with clear value propositions for all participants.

Lessons Learnt

The lessons from these large-scale pilots are clear: the technology works, cross-border interoperability is achievable, and the security frameworks can protect user privacy. Yet technology alone is insufficient.

Success requires treating the wallet not as a compliance exercise but as a transformative opportunity to redefine digital experiences.

The pilots have demonstrated both the promise and complexity of deploying a truly European digital identity solution.

The question now is whether Europe can act collectively to address the governance gaps, align regulatory frameworks, establish viable business models, and build the trust necessary to move from successful pilots to sustained adoption.

The foundations have been laid; the next phase will determine whether Europe can deliver on the vision of a secure, interoperable, and trusted digital identity ecosystem for all its citizens.

The following pages take a deeper dive into the final reports published by EWC, POTENTIAL, NOBID and DC4EU, representing 550+ organisations from 26 EU member states together with Norway, Iceland and Ukraine.

The foundations have been laid; the next phase will determine whether Europe can deliver on the vision

The ambitious target is to achieve 80% of EU citizens with access to the EU Digital Identity Wallet by 2030. The critical insights from Europe's largest Digital Identity experiment provide a roadmap to developing citizen-centric ecosystems over the next three years.

Pilot 1

**EWC Consortium
Travel &
Payments**

Pilot 1: EWC Consortium

The EWC consortium completed the largest test of EUDI wallets across travel and payment scenarios. Here's what happened when 300+ people across the EU tried to use digital wallets for their actual journeys.

Austria	Denmark	Greece	Netherlands	Spain
Belgium	Estonia	Hungary	Norway	Sweden
Bulgaria	Finland	Ireland	Poland	Ukraine
Croatia	France	Italy	Romania	United Kingdom
Czech Republic	Germany	Luxemburg	Switzerland	

VISA   **amadeus**   **AEGEAN »**   **RDE**   **SICPA**
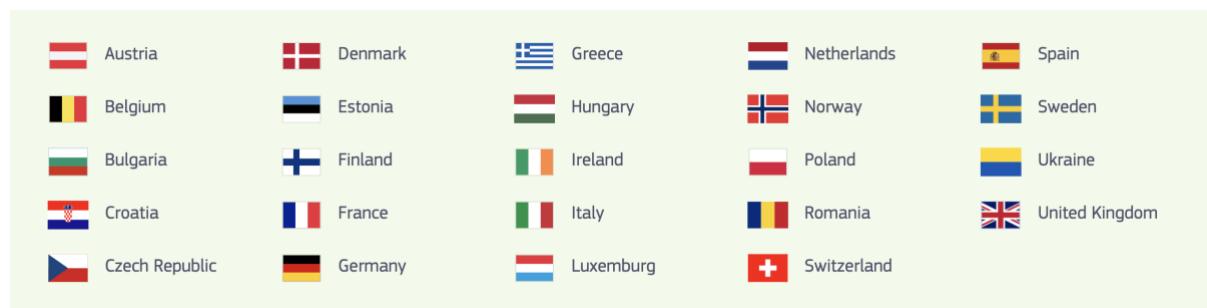
🧪 What Was Actually Tested

Under the leadership of the use case owners Visa, Amadeus, Aegean, RDE and SICPA, four live use cases were tested with real transactions:

- Ferry ticket purchase - complete journey from payment to boarding with digital credentials.

- Museum visits - age verification for discounts, digital tickets, seamless entry.

- Airline check-in - automated passenger information with consent-based photo sharing.

- Hotel registration - instant form filling that took seconds instead of minutes.

Can the EUDI Wallet Actually Work for Travel and Payments?

✅ What Worked

The good news is that production-ready transactions were completed.

- Real ferry tickets purchased with integrated payment.

- Actual boarding passes issued and verified.

- Live passenger data shared with airlines (Lufthansa tested with hundreds of customers).

- Hotel check-ins automated with regulatory compliance.

- Age verification without oversharing personal data.

> **The good news:** The infrastructure is ready. The integrations are possible. The technology delivers.

💡 What Needs Improvement

After surveying 9,000+ EU citizens, only 29% would adopt the wallet today.

Why the gap?

- Citizens ask "what's in it for me?" - not "what's good for the EU?"

- Existing solutions work "well enough" for most people.

- Security concerns outweigh perceived benefits.

- Trust deficit is the real barrier, not technical capability.

> **The insight:** The wallet must redefine digital experiences, not just replicate them.

🧭 The Path Forward for the Ecosystem

Five critical lessons learned:

1. Focus on where current solutions fail, not where they're adequate.

2. High-frequency, high-value use cases drive adoption.

3. Business models must work for all public and private participants.

4. User experience must exceed current benchmarks, not match them.

5. Building trust requires consistent delivery, not just promises.

> **The path forward:** Demonstrate transformative value through everyday use cases.

To read more about the EWC Consortium including the final report visit:
https://eudiwalletconsortium.org/
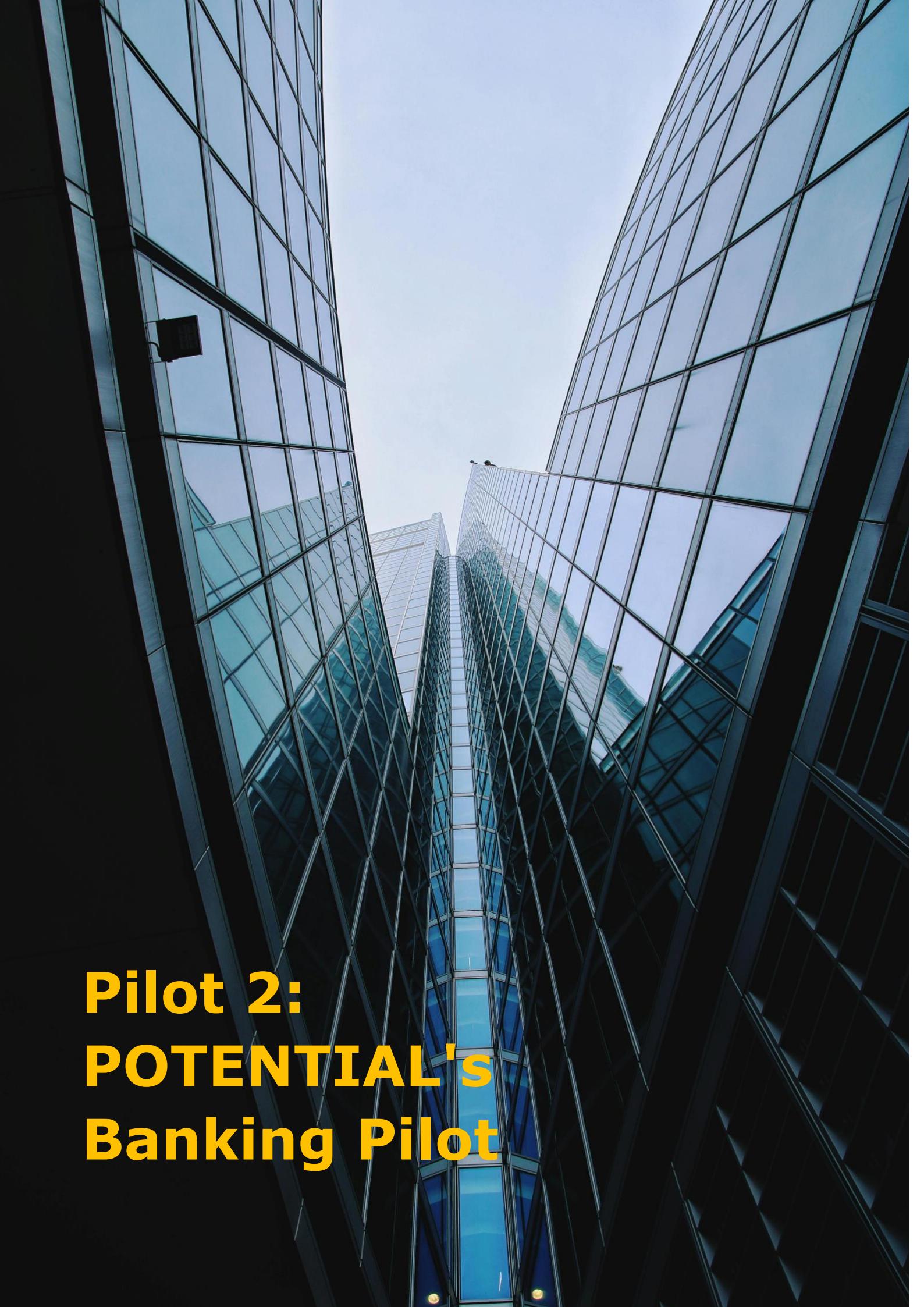
Pilot 2: POTENTIAL's Banking Pilot

Pilot 2: POTENTIAL's Banking Pilot

The POTENTIAL consortium completed one of the most comprehensive tests of EUDI wallets across government, banking, telecom, mobility, trust services, and healthcare.

The pilot focused on proving whether EUDI Wallets could streamline Know-Your-Customer (KYC) and Anti-Money Laundering (AML) processes whilst meeting strict regulatory requirements across 19 Member States and Ukraine.

Can EUDI Wallets Actually Simplify Bank Onboarding?

This was one of six use cases designed to validate the wallet's readiness for production deployment between 2026-2027.

🇦🇹 Austria	🇫🇮 Finland	🇮🇹 Italy	🇵🇹 Portugal
🇧🇪 Belgium	🇫🇷 France	🇱🇹 Lithuania	🇸🇰 Slovakia
🇨🇾 Cyprus	🇩🇪 Germany	🇱🇺 Luxemburg	🇸🇮 Slovenia
🇨🇿 Czech Republic	🇬🇷 Greece	🇳🇱 Netherlands	🇪🇸 Spain
🇪🇪 Estonia	🇭🇺 Hungary	🇵🇱 Poland	🇺🇦 Ukraine
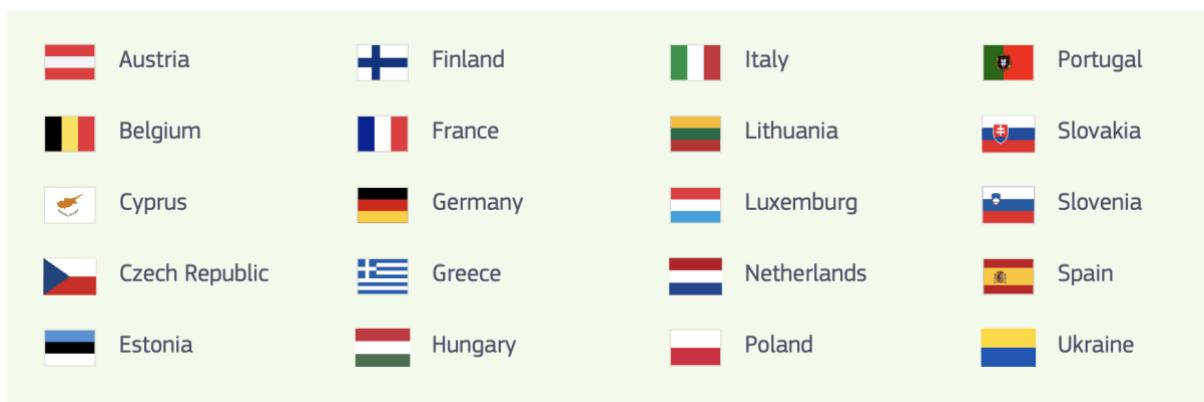
🧪 What Was Actually Tested

Under the leadership of participating Member States and over 140 partners, six live use cases were tested with real transactions:

1. eGovernment services - identification, legal representation, and proof of residence.

2. Bank account opening - customer onboarding with PID, residence, and tax ID attestations.

3. SIM card registration - secure mobile service activation and fraud prevention.

4. Mobile driving licence - digital mDL for car rentals and police checks.

5. Qualified e-Signatures - legally valid digital signing integrated into wallets.

6. ePrescription - cross-border pharmacy services with Health ID credentials.

✓ What Worked

The good news is that production-ready transactions were completed.

- Real cross-border government service access with wallet attestations.

- Actual bank accounts opened using wallet-based KYC/AML compliance.

- Live SIM cards registered with wallet PID and MSISDN issuance.

- Mobile driving licences verified in both proximity and remote settings.

- Qualified electronic signatures created directly in wallets.

- First-ever cross-border online pharmacy transactions with Health ID.

- Banks that committed early demonstrated measurable efficiency gains.

> **The good news:** The infrastructure is ready. Cross-border interoperability is proven. The technology delivers.

💡 What Needs Improvement

After 1,300+ interoperability tests, technical feasibility is confirmed but challenges remain:

- Differences in standards adoption across Member States.

- Fragmented certification approaches and varied implementations of the European Architecture and Reference Framework (ARF) .

- Delays in secure element specs slowed adoption.

- Governance gaps in public-private collaboration models.

- AML regulations don't explicitly recognise wallet attestations—creating legal uncertainty for financial institutions.

- Liability frameworks are unclear, banks need certainty on responsibility when relying on wallet credentials.

> **The insight:** Tech works, but regulatory and liability frameworks lag and sustainable business models still unclear.

🧭 The Path Forward for the Ecosystem

Five critical lessons learned:

1. Interoperability is achievable but fragile - only with strict EU-wide standards.

2. Governance determines success - strong national coordination plus EU-level forums.

3. User trust is fragile - Privacy-by-Design and consistent UX are essential.

4. Security needs early frameworks - certification and liability must be embedded from the start.

5. Scale and inclusivity matter - EU support needed so all Member States progress together.

> **The path forward:** Accelerate ARF alignment, establish mandatory conformance testing, prioritise user-centric design.

📋 POTENTIAL's Recommendations

The POTENTIAL final report made a set of recommendations for 2026-2027 roadmap:

- Mandate wallet acceptance for KYC/AML across all EU banks to drive adoption.

- Harmonise AML regulations to explicitly accept wallet-based attestations.

- Develop open-source connectors to reduce integration barriers.

- Clarify liability frameworks before requiring widespread adoption.

- Enable reuse of financial attestations (IBAN, tax ID, MSISDN) across institutions Success requires coordinated action across regulators, banks, and technology providers

To read more about the POTENTIAL Consortium including the final report visit: https://digital-identity-wallet.eu

Pilot 3: NOBID's Cross-Border Banking & Identity Pilot

Pilot 3: NOBID's Cross-Border Banking & Identity Pilot

The NOBID consortium brought together 5 countries (Norway, Iceland, Italy, Denmark, and Latvia) to test EUDI Wallets across real cross-border scenarios with over 140 partners.

The pilot validated wallet functionality across multiple use cases including cross-border bank account opening, higher education credentials, mobile driving licenses, age verification, and digital signatures.

Is Cross-border digital identity more than just a technical challenge?

Testing involved both Model A (common wallet) and Model B (national wallet) implementations to prove interoperability between different architectural approaches.
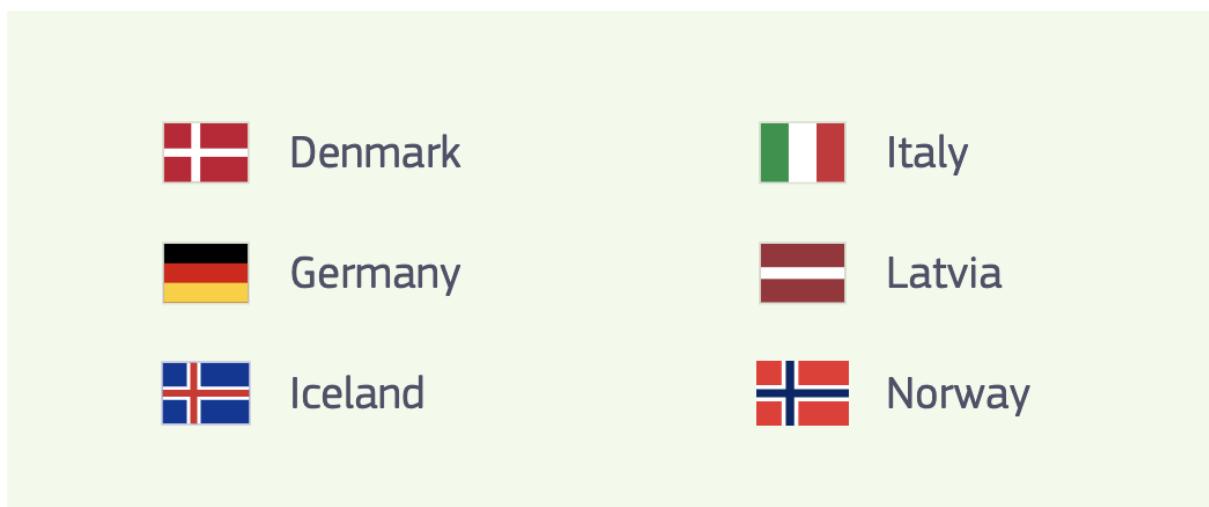
🧪 What Was Actually Tested

Led by participating Member States and payment authorities, six core use cases were validated with real users:

1. Cross-border bank account opening - Norwegian citizens opening accounts in Italy using PID and fiscal code attestations.

2. Higher education credentials - Universities issuing and verifying diplomas across borders (Latvia, Italy, Lithuania, Estonia).

3. Mobile driving licenses - Issuing and verifying mDLs in both proximity and remote settings.

4. Age verification - Cross-border age checks (Icelandic PID verified in Norway).

5. Digital signatures - Qualified e-signatures and parental representation scenarios.

6. Identity matching - Creating national identifiers for foreign residents to access local services

✅ What Worked

The good news: technical interoperability was proven across national borders.

- Model A and Model B wallets successfully interoperable - proving different architectural approaches can work together.

- Real cross-border credentials issued and verified - Norwegian PID used to obtain Italian fiscal codes; Latvian diplomas verified in Italy.

- Multiple authentic sources connected - Universities, transport authorities, banks, and public registries all successfully issued credentials.

- Age verification worked seamlessly - Icelandic citizens proved age eligibility in Norway with minimal data sharing.

- Privacy-preserving flows validated - selective disclosure working as intended (e.g., sharing only "over 18" not full birth date).

> **The good news:** The infrastructure works. Cross-border technical interoperability is achievable.

💡 What Needs Improvement

After extensive testing across five (5) countries, semantic and procedural challenges remain:

- Constant standard evolution disrupted development - ARF, RI, and OpenID4VC specs updated frequently, causing version mismatches between partners.

- Semantic interoperability is fragile - no common data models for addresses, diplomas, or citizen data across Member States.

- User experience gaps identified - confusing multi-step flows, unclear data sharing requests, language barriers, and accessibility issues for persons with special needs.

- Legal complexity in representation - parental authority, guardianship, and business representation differ significantly between countries.

- Missing business models - unclear who pays for wallet operations when end-users access it for free.

> **The insight:** Technology is ready. However, standards alignment, semantic harmonisation, and user-centric design are the critical path forward and need continued work.

The Path Forward for the Ecosystem

Five critical lessons resulted from the Nordic-Baltic cross-border testing:

1. Stable standards are non-negotiable - freeze core specifications early and maintain backward compatibility during pilots.

2. Semantic rulebooks essential - especially for education, addresses, and representation credentials.

3. User trust requires clarity - multilingual support, transparent data sharing, and robust authentication (not just PIN codes).

4. Accessibility cannot be afterthought - testing revealed significant barriers for persons with special needs.

5. Cross-LSP collaboration accelerates learning - coordination between NOBID, POTENTIAL, and DC4EU advanced interoperability faster.

> **The path forward:** Prioritise semantic interoperability, invest in user experience, establish sector-specific data models.

☑️ NOBID's Recommendations

The NOBID consortium's roadmap for 2026-2027:

- Establish stable, versioned standards - clear ARF releases with defined upgrade paths.

- Develop sector-specific rulebooks - starting with education (coordinate with DC4EU) and citizen data.

- Harmonise legal frameworks for representation - parental authority, guardianship, and business mandates.

- Invest in inclusive design - prioritise accessibility, multilingual interfaces, and clear user guidance.

- Define sustainable business models - clarify who pays for authentication, issuance, and verification.

- Expand cross-border testing - continue pilot collaborations to validate semantic alignment.

Success requires coordinated action across Member States, regulators, and technology providers.

To read more about the NOBID Consortium including technical reports visit: https://www.nobidconsortium.com/NOBID

Pilot 4: DC4EU's Education & Social Security

Pilot 4: DC4EU's Education & Social Security Pilot

The DC4EU Consortium brought together 101 organisations from 25 countries (22 EU Member States, Norway, Switzerland, and Ukraine) to test EUDI Wallets across education and social security domains with over 140 stakeholders.

The pilot validated wallet functionality for educational credentials and professional qualifications in the education sector, and the Portable Document A1 (PDA1) and European Health Insurance Card (EHIC) in the social security sector.

Can EUDI Wallets Transform Education Credentials and Social Security Across Europe?

Testing involved comprehensive pilots with universities, social security institutions, health care providers, and public administrations to prove cross-border interoperability.

Austria	France	Italy	Norway	Sweden
Belgium	Germany	Lithuania	Poland	Ukraine
Czech Republic	Greece	Luxemburg	Portugal	
Denmark	Hungary	Malta	Romania	
Finland	Ireland	Netherlands	Spain	

⚗️ What Was Actually Tested

Led by participating Member States, social security authorities, and educational institutions, four core use cases were validated with real users:

1. Educational credentials - Universities issuing and verifying diplomas and professional qualifications across borders with full data control and cross-border recognition.

2. Portable Document A1 (PDA1) - Digital credentials proving social security coverage when working abroad, streamlining cross-border employment verification.

3. European Health Insurance Card (EHIC) - Digital EHIC issuance and verification enabling citizens to access healthcare services across borders.

4. EBSI integration - First Large-Scale Pilot to utilise European Blockchain Services Infrastructure (EBSI) at scale as a trusted data source for the EUDIW.

✓ What Worked

The good news: technical interoperability was proven across education and social security domains.

- Real educational credentials issued - Universities successfully issued digital diplomas and professional qualifications with seamless cross-border verification.

- Social security credentials digitised - PDA1 and EHIC successfully issued and verified in demo wallets, proving feasibility for mobile workers and travellers.

- EBSI integration validated - Hybrid trust model combining eIDAS framework with EBSI-anchored verifiable data registries demonstrated successfully.

- Open-source architecture developed - Comprehensive interoperability lab created for testing and integration, supporting ecosystem expansion.

- Privacy-preserving flows confirmed - Selective disclosure working as intended, giving citizens full control over their personal data.

> **The good news:** The infrastructure works. Cross-border credential exchange in education and social security is achievable.

What Needs Improvement

After extensive testing across 25 countries, technical and procedural challenges remain:

- Standard evolution disruption as the ARF and OpenID4VC specifications continued to be updated frequently during development, causing version mismatches and integration delays.

- Semantic interoperability gaps as there were no common data models for educational credentials, social security documents, or citizen data across Member States.

- User experience complexity was observed due to confusing multi-step flows, unclear data sharing requests, and accessibility barriers for persons with disabilities identified.

- Technical complexity communication highlighted the need for layered content approach ("For Experts" vs. "For Everyone") in order to reach broader audiences.

- Business model uncertainty due to unclear and/or sustainable funding mechanisms for wallet operations, credential issuance, and verification services.

> **The insight:** Technology readiness confirmed. Standards stability, semantic harmonisation, and user-centric design are the critical path forward.

The Path Forward for the Ecosystem

Five critical lessons from DC4EU's cross-border testing:

1. Freeze core specifications early. Aim for stable, versioned standards with backward compatibility during pilots to prevent development disruption.

2. Establish sector-specific rulebooks. Education credentials and social security documents require domain-specific data models and governance frameworks.

3. Prioritise inclusive design. Multilingual interfaces, accessibility for persons with special needs, and transparent data sharing are non-negotiable.

4. Leverage EBSI for hybrid trust. The combination of eIDAS trust framework with EBSI-based registries enabled enhanced security for non-qualified attestations.

5. Sustain cross-LSP collaboration. Coordination with EWC, NOBID, and POTENTIAL accelerated learning and prevented duplication. This highlighted the value of the pilots.

> **The path forward:** Build on proven technical foundation, invest in semantic interoperability, establish sustainable business models.

☑ DC4EU's Recommendations

The DC4EU consortium's roadmap for the ecosystem:

- Stable standards with clear versioning. Defined ARF releases with explicit upgrade paths and backward compatibility guarantees.

- Domain-specific governance frameworks. Develop sector rulebooks for education and social security coordinated across LSPs and Member States.

- Semantic interoperability investment. Need for common data models, ontologies, and linked data formats (JSON-LD) for automated processing.

- Accessibility and multilingual support. Inclusive design principles embedded from the start, not retrofitted.

- Sustainable business models. Clear cost allocation for authentication, issuance, verification, and wallet operations.

- Open-source ecosystem enablement. Continued development of interoperability labs and testing frameworks for stakeholder integration.

Importantly, success requires coordinated action across Member States, educational institutions, social security authorities, and technology providers.

To read more about the DC4EU Consortium including technical reports visit: https://dc4eu.eu

About Meeco

Meeco is a leading provider of digital identity infrastructure, enabling organisations to build secure, standards-based identity solutions that put citizens in control of their personal data.

With operations in Australia, Belgium, and the UK, Meeco has been at the forefront of the digital identity transformation, working with governments, enterprises, and consortia to deliver production-ready systems that balance privacy, security, and usability.

SVX Platform: Bridging Pilots to Production

The learnings from the EUDI Large Scale Pilots (EWC, POTENTIAL, NOBID, and DC4EU) have validated the technical feasibility of Europe's digital identity vision.

However, as these pilots consistently demonstrated, technical capability alone doesn't guarantee adoption. The gap between successful proof-of-concepts and scalable production deployment requires infrastructure that addresses the real-world complexities uncovered during these tests.

This is precisely where Meeco's Secure Value Exchange (SVX) Platform operates. SVX provides the orchestration layer that connects wallets, credentials, and services into coherent experiences that organisations can deploy with confidence.

Rather than building from scratch, organisations can leverage SVX's comprehensive support for the latest digital credential standards, including the final versions of OpenID4VCI and OpenID4VP, IETF SD-JWT VC, and ISO Mobile Documents, reducing the complexity that plagued many pilot implementations.

Addressing the Challenges Identified in the Pilots

The Large-Scale Pilots revealed critical challenges that must be solved for successful adoption:

Standards Complexity: The pilots highlighted constant standard evolution as a major disruptor, with frequent ARF, Reference Implementation, and OpenID4VC updates causing version mismatches.

- SVX provides RESTful API's for all its functionalities which enables organisations to leverage standards compliance while keeping business logic in existing systems. This separation of concerns simplifies integration and deployment without forcing wholesale system replacement.

Integration Friction: POTENTIAL, NOBID, and DC4EU all identified integration complexity as a barrier to adoption.

- ☑ SVX's Resource Hook Integration enables organisations to leverage standards compliance while keeping business logic in existing systems. This separation of concerns simplifies deployment without forcing wholesale system replacement.

User Experience Gaps: All four pilots emphasized that user experience must exceed current benchmarks, not merely match them.

- ☑ SVX Verify exemplifies this principle, providing a hosted identity verification service that makes high-assurance identity exchange accessible in minutes rather than months, with built-in privacy controls and multi-language support.

Governance and Business Model Uncertainty: The pilots consistently raised questions about who pays for wallet operations, credential issuance, and verification services.

- ☑ SVX's flexible deployment model, supporting both wallet-based credentials and account-based identity providers, enables organisations to implement sustainable business models while maintaining interoperability.

Making Standards-Based Identity Practical

The technical complexity required for secure, privacy-preserving digital credentials doesn't need to translate into deployment complexity. SVX demonstrates this principle through features like self-service sandbox access, unified JSON-based configuration with automatic validation, and comprehensive developer documentation. Organisations can implement production-ready identity verification workflows without becoming standards experts themselves.

As Member States face November 2026 deployment deadlines and private sector acceptance requirements by December 2027, the transition from pilot to production demands infrastructure that works today while remaining adaptable for tomorrow's ecosystem evolution. SVX provides this bridge, enabling organisations to deliver immediate value through integration with existing identity providers while building future readiness for emerging wallet-based credentials.

The EUDI Large Scale Pilots have laid the foundation. The path forward requires tools that make implementation practical, sustainable, and user centric. Meeco's SVX Platform is purpose-built for this transition, helping organisations move from successful pilots to trusted, adopted digital identity ecosystems.

Learn more about Meeco and the SVX Platform: www.meeco.me