Potential
For European Digital Identity

Co-funded by
the European Union

POTENTIAL: FOR EUROPEAN DIGITAL IDENTITY

Main findings, lessons learned and recommendations

This document is intended for Government Authorities, Regulators, Policymakers, Service Providers, and Relying Parties.

September 2025

1. Executive Summary

The POTENTIAL project is one of four EU Large-Scale Pilots under the Digital Europe Programme, tasked with validating the deployment of the European Digital Identity Wallet (EUDI Wallet) across six use cases: e-Government services, bank account opening, mobile SIM card registration, mobile driving licence (mDL), qualified e-Signature, and e-Prescription. The pilot brought together over 140 partners from 19 Member States and Ukraine, conducting more than 1.300 interoperability tests and 1.000 successful transactions, including 249 cross-border scenarios. These results provide essential insights for the rollout of EUDI Wallets under the amended eIDAS Regulation (eIDAS 2.0) between 2026 and 2027.

Vilnius Interop Event (May 2025)

Board of Beneficiaries Prague (June 2025)

2. Purpose & Audience

This document provides a strategic summary of the POTENTIAL pilot project, highlighting lessons learned, strategic recommendations, and key implications for policy and governance. It is intended for Governments, regulators, policymakers, relying parties, and private sector actors who will play a role in the design, implementation, and adoption of national EUDI Wallets.

- Participants: 140+ partners, 19 Member States + Ukraine, 6 Use Cases tested
- Testing Achievements: 1,300+ tests, 1,000+ successful transactions, 249 cross-border scenarios
- Use Cases: e-Government, Bank Account Opening, SIM Registration, mobile driving licence, e-Signature, e-Prescription
- Strategic Outcomes: Validated interoperability, governance lessons, security insights, and user trust factors
- Next Steps: to adopt further ARF, Wallet Reference Implementation, establish a legal framework of eIDAS Regulation and Implementing Acts for EUDI Wallet rollout (2026–2027).

3. Recommendations for Government Authorities

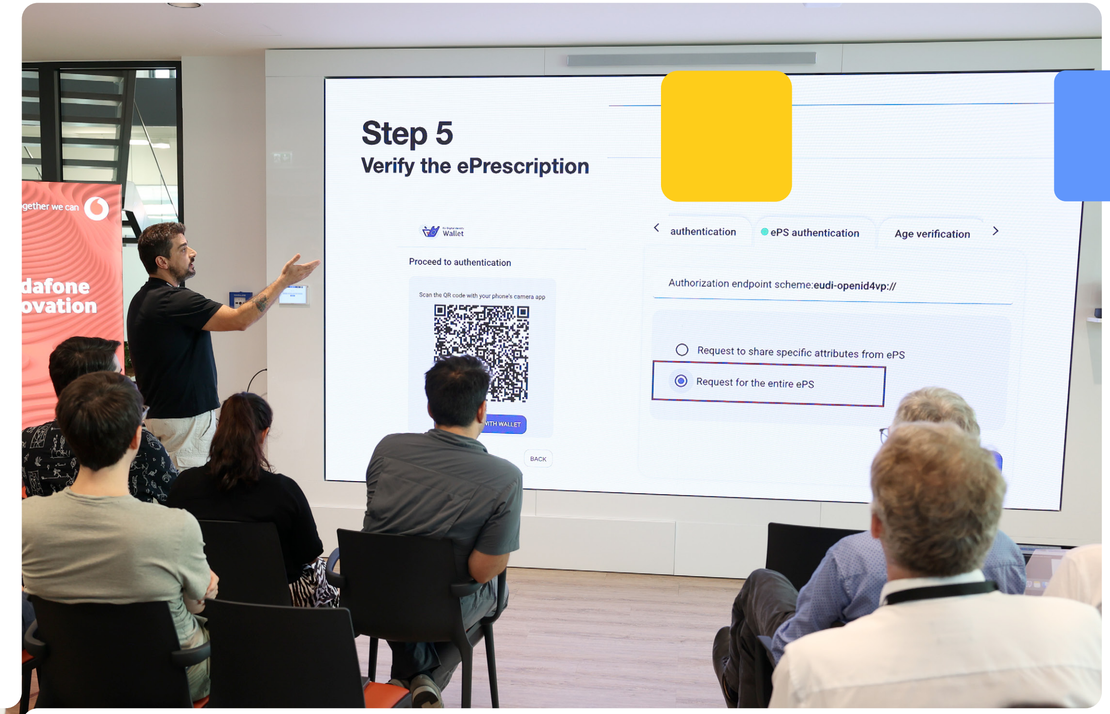
Strategic recommendations emerging from the POTENTIAL pilot underscore the need for coherence, scalability, and long-term sustainability of the EUDI Wallet ecosystem.

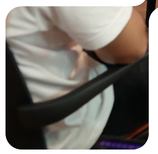
1. National governments should prioritize early alignment with EU frameworks to reduce future rework, invest in shared testing infrastructures, and coordinate funding streams to support large-scale deployment. The pilots demonstrated that without strong political leadership, wallet adoption risks being fragmented and delayed. National strategies should include a clear roadmap, backed by resources and a communication plan to build awareness among citizens and businesses.

- Align national wallet initiatives with the European Architecture and Reference Framework (ARF) and Implementing Acts.
- Leverage pilot infrastructure and methodologies to reduce duplication and accelerate national deployment.
- Encourage collaboration between Member States to promote mutual learning and convergence.

2. Governance is central to the success of EUDI Wallets. The pilots demonstrated that Member States with dedicated coordination bodies and strong inter-ministerial collaboration made progress more quickly. Future governance structures should incorporate both regulatory oversight and operational management. Public-private partnerships are essential: banks, telecom operators, and trust service providers must be involved from the outset. EU-level coordination mechanisms, such as a permanent forum for Member States and the EC, should ensure shared roadmaps, common certification schemes, and synchronized implementation schedules.

- Establish a dedicated governance body at the national level with clear responsibility for wallet implementation.
- Promote public-private collaboration models as tested in POTENTIAL.
- Ensure continuous engagement with the European Commission and peer Member States.
- Clarify a sustainable business model for both public and private stakeholders





Potential Hackathon Dresden (August 2024)

Board of Beneficiaries Prague (June 2025)

3. Interoperability remains the cornerstone of the EUDI Wallet vision. POTENTIAL's cross-border pilots proved technical feasibility but also highlighted gaps: differences in standards adoption, fragmented certification approaches, and varied levels of ARF implementation. Future wallet ecosystems must adopt a rigorous and harmonised compliance framework that covers protocols, data schemes, secure elements, and liability rules. Testbeds such as the Playground used in POTENTIAL should evolve into a European-level conformance environment, mandatory for all wallet solutions before market entry. In addition, strong change management and backwards compatibility mechanisms must be established, since protocols and standards evolve continuously. Such governance should be coordinated at the EU level, beyond national initiatives, to ensure sustainable interoperability across Member States.

- Adopt EU-wide standards to ensure interoperability, based on lessons from the series of interoperability testing workshops across the EU.
- Anticipate evolving requirements from eIDAS 2.0 Implementing Acts and prepare early alignment.
- Ensure technical solutions integrate secure elements and certification frameworks.

4. Adoption will ultimately determine the success of the EUDI Wallet. The pilots demonstrated that users value simplicity, transparency, and control over their data. Citizens expressed concern about complex onboarding and inconsistent user interfaces across Member States. To address this, UX guidelines at the EU level must be defined, ensuring consistency and accessibility. Communication campaigns explaining wallet benefits in everyday scenarios (banking, healthcare, travel) are critical to building trust. Engagement of the private sector is equally vital, as widespread acceptance by banks, telecoms, and online services will determine whether citizens find the wallet useful beyond government portals.

- Prioritise user experience and citizen-centric design, including selective disclosure and multilingual support.
- Engage private sector stakeholders, especially banks, telecoms, and healthcare providers, early in adoption planning.
- Build public trust through transparency, clear communication, and robust data protection guarantees.

Warsaw Interop Event (February 2025)

4. Five Strategic Insights

The POTENTIAL generated a wealth of lessons on interoperability, governance, security, adoption, and inclusivity. These five insights should guide policymakers as they move from pilots to full deployment:

1. **Interoperability is achievable, but fragile.**
   Cross-border tests proved that wallet solutions can work across Member States, but only with strict adherence to common standards. Divergent adoption of specifications led to delays, duplication, and higher costs. EU-wide conformance testing must be mandatory before market rollout.

2. **Security is as much about governance as technology.**
   Delays in secure element specifications slowed adoption. Without early certification and liability frameworks, risks multiply. Embedding governance into security from the start will be essential for trust.

3. **Governance determines success.**
   Member States with strong national coordination bodies and inter-ministerial collaboration advanced fastest. Multi-layered governance — strong national leadership plus EU-level coordination — is critical. Public–private collaboration must be institutionalised, not ad hoc. A global and sustainable business model for both public and private stakeholders could not be clarified and is still missing.

4. **User trust is fragile.**
   Citizens value privacy and control but worry about data over-collection and inconsistent user interfaces. UX and transparency matter as much as compliance. Wallet adoption will fail without privacy-by-design, selective disclosure, and consistent design standards. Private wallet solutions will further compete for adoption by the users.

5. **Scale and inclusivity matter.**
   Smaller Member States and Ukraine benefited from knowledge-sharing but faced resource gaps. EU support mechanisms are needed to ensure all Member States progress together. Fragmentation risks undermining the entire project.

5. Six POTENTIAL use cases

To validate the European Digital Identity Wallet in real-world settings, the POTENTIAL project piloted six diverse use cases across government, finance, telecom, mobility, trust services, and healthcare. Together, these domains cover the key sectors where citizens and businesses most often rely on identity, authentication, and credentials in cross-border contexts.
Each use case tested the wallet's technical feasibility, legal alignment, and policy implications, while engaging a wide range of Member States and industry partners. The insights gathered provide a blueprint for the large-scale adoption of the EUDI Wallet across Europe.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Use Case 1 eGovernment Services

Overview of involved partners per Member States

14 countries participated: **AT, BE, CZ, DE, EL, FI, FR, IT, LU, NL, PL, PT, SI, UA.** Both credential issuers and relying parties were involved, ensuring tests reflected diverse legal, technical, and administrative contexts.

Objectives and context

The pilots tested wallet-based identification and authentication for natural and legal persons, including legal representation and proof of residence. The goal was to assess interoperability, scalability, and citizen usability in cross-border eGovernment services, while also exploring integration with the Once Only Technical System (OOTS).

Key results

UC1 successfully piloted four cross-border scenarios and developed attestation rulebooks for Powers of Representation, Company Registration, and Certificates of Residence. A study on using a Legal Person wallet outlined four possible models for future adoption. Tests confirmed the feasibility of using SD-JWT and mDoc standards across government contexts.

Technical recommendations

- Develop EU-wide testbeds and documentation to avoid divergent implementations.
- Deliver a robust EU-level solution for identity matching across Member States.
- Ensure consistent use of SD-JWT and mDoc standards.
- Provide open-source integration components for Relying Parties and Issuers.

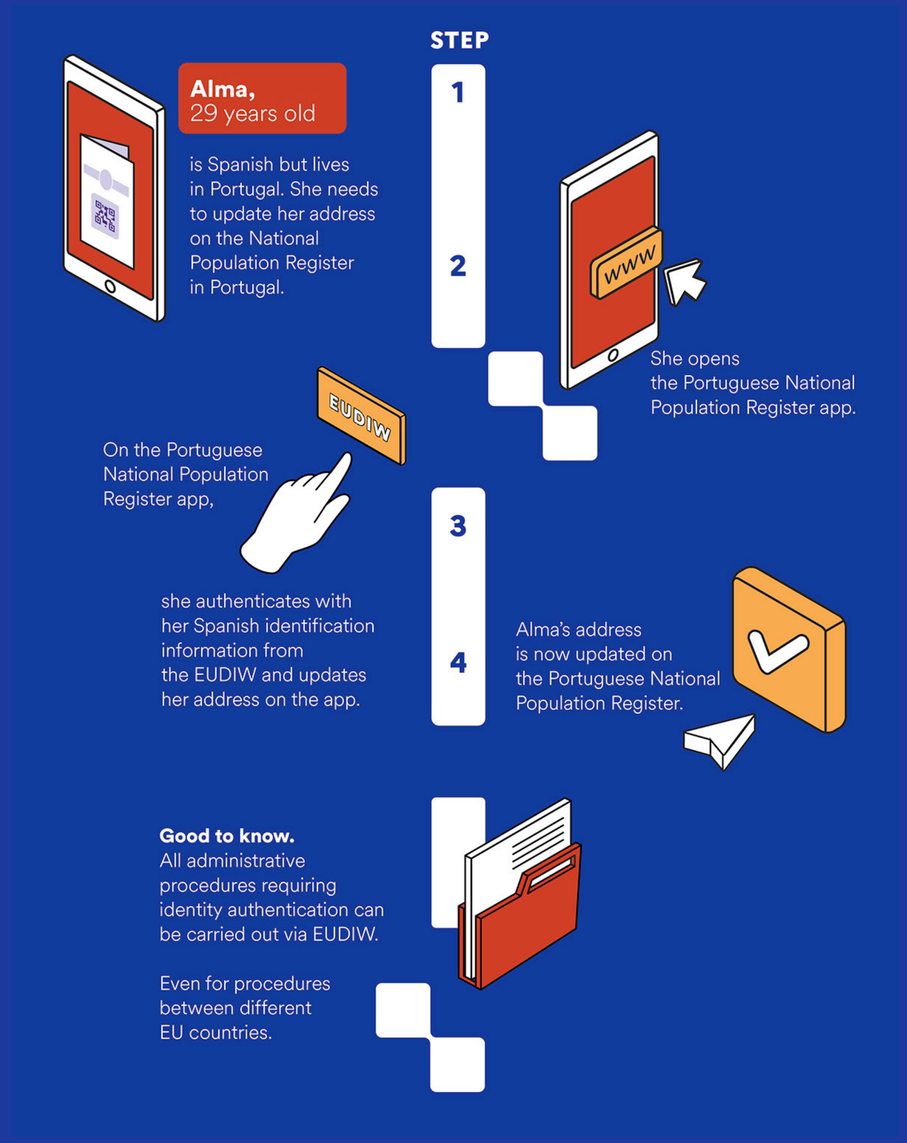
Legal recommendations

- Clarify legal frameworks for representation, company data, and residence certificates.
- Define safeguards for consent and liability in cross-border use.
- Embed attestation rulebooks into Implementing Acts and ARF guidance.

Policy recommendations

- Establish a governance and certification framework covering wallets, Relying Parties, and attestations.
- Provide early access to stable specs and roadmaps to Member States.
- Promote cross-border reuse of standardized attestations.
- Support structured public–private collaboration with dedicated resources.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY



POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Use Case 2 Bank Account Opening

Overview of involved partners per Member States

17 countries participated, of which 8 served as RPs: **AT, BE, CZ, DE, EE, EL, FR, FI, HU, IT, LU, LT, NL, PL, PT, SI, UA**, involving wallet providers, financial institutions, and regulators.

Objectives and context

The pilots focused on wallet credentials for customer onboarding in banking. Scenarios included PID, residence, MSISDN, and tax ID attestations, as well as Qualified Electronic Signatures (QES) for AML/KYC compliance.

Key results

UC2 demonstrated that the EUDI Wallet can streamline onboarding, though challenges remain around regulatory harmonisation and QES flows. While adoption was uneven, the pilots provided critical insights into how AML compliance and wallet integration can be reconciled at the EU level.

Technical recommendations

- Support issuance and exchange of financial attestations (IBAN, tax ID, MSISDN).
- Provide open-source wallet connectors for bank onboarding systems.
- Align wallet onboarding with AML/KYC technical standards.

Legal recommendations

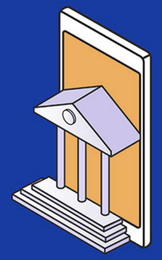
- Harmonise AML regulations to explicitly accept wallet-based attestations.
- Clarify liability for financial institutions relying on wallet credentials.
- Ensure recognition of QES flows for onboarding under eIDAS 2.

Policy recommendations

- Require banks across the EU to accept wallets for KYC/AML.
- Provide regulatory guidance for wallet integration into financial services.
- Promote reuse of attestations across the financial sector.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

How to open a bank account with an EU digital identity wallet?



Ulrike,
38 years old

Needs to open
a new bank account
to expand
her business.

STEP

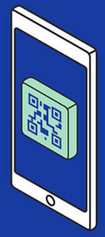
1

2

On the bank app,
or at the bank

she chooses the EUDIW to identify herself, instead of giving an ID copy.

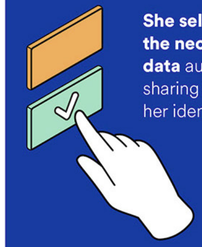
Ulrike opens her EUDIW by clicking on the deep link suggested or scans a QR code presented by the bank officer.



3

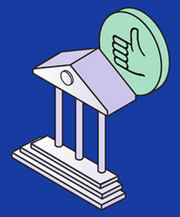
4

5



She selects the necessary data authorizes sharing to prove her identity.

The bank receives automatic verifications without handling sensitive data **Ulrike confirms the authorization to share her data.**



And now,
Ulrike gets her new bank account!

6

The bank sends
the general terms
& conditions documents
and **Ulrike uses the wallet to officially e-sign it.**

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Use Case 3 SIM Card Registration

Overview of involved partners per Member States

7 countries participated: **AT, DE, CZ, EL, FR, PL, UA,** with telecom operators, wallet providers, and regulators.

Objectives and context

The pilots explored wallet-based PID identification for secure SIM card registration and fraud prevention, and issuing of MSISDN attestations. They assessed interoperability with telecom requirements and the feasibility of wallet adoption in large-scale user flows.

Key results

UC3 showed wallets can enable fast and secure online onboarding for telecom users and provide tangible benefits for Mobile Service Providers and their customers. Relying Parties stressed that the maturity of the EUDI-Wallet system infrastructure and, in some member states, regulatory recognition are essential for mass adoption.

Technical recommendations

- There should be an iterative update planning for developing the EUDI-Wallet infrastructure at the EU-level.
- The global interoperability test and release concept for mobile devices could be used as a blueprint for wallet interoperability at the EU scale.
- Wallet system operations and support could benefit from telecom expertise in system operations.
- Resolutions for detected onboarding obstacles affecting Relying Parties and supporting measures for early adopters should be implemented.

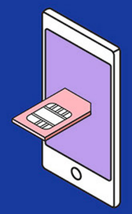
Legal recommendations

- Align telecom regulations to accept wallet-based registration.
- Clarify liability for telecom operators using wallet attestations.
- Ensure compliance with national fraud-prevention rules.

Policy recommendations

- Invite Mobile Service Providers to participate in the national preparations for the wallet introduction.
- Support Mobile Service Providers in pilot-to-production transition.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY



Nikos,
56 years old

Needs a new SIM card for his mobile phone because he just moved to Belgium.

STEP

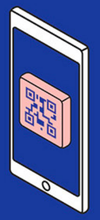
1

2

In-store
or online

he chooses the EUDIW to identify himself, instead of giving an ID copy.

Nikos opens his EUDIW by clicking on the deep link suggested or scans a QR code presented by the telephone operator.



3

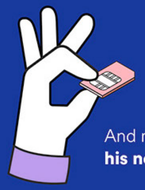
4

He selects the necessary data authorizes sharing to prove his identity.

5

The telephone operator receives automatic verifications without handling sensitive data.

Nikos confirms the authorization to share his data.



And now, **Nikos gets his new SIM card!**

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Use Case 4 Mobile Driving Licence (mDL)

Overview of involved partners per Member States

16 countries participated: **AT, BE, CZ, DE, EE, FI, FR, ES, EL, IT, LU, LT, NL, PL, PT, UA,** working alongside ISO standardisation bodies.

Objectives and context

UC4 tested wallet-based mDLs in proximity and remote settings, including car rentals and police checks. It also explored revocation mechanisms and lifecycle management, aiming for EU and global interoperability based on ISO 18013-5/7.

Key results

Pilots validated mDL use across borders and highlighted challenges in offline verification and UX design. UC4 showed that mDLs can serve as a flagship use case, provided common standards are consistently applied.

Technical recommendations

- Align implementations with ISO 18013-5/ 7 and ARF profiles.
- Ensure robust offline verification support.
- Provide open-source verifier modules for law enforcement and mobility.

Legal recommendations

- Define liability frameworks for verification failures.
- Clarify revocation and validity rules in cross-border contexts.
- Ensure legal recognition of mDLs as ID across the EU.

Policy recommendations

- Recognise mDLs as valid ID documents EU-wide.
- Promote common technical and UX standards.
- Integrate mDLs with mobility services (car rental, transport platforms).

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Amir,
42 years old

Needs to use a carsharing service or rent a car for his holiday in Italy.

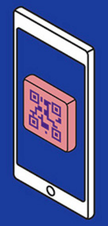
STEP 1

He chooses the EUDIW to prove his right to drive,

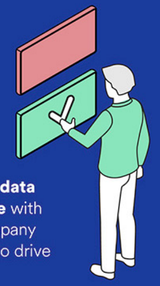
instead of showing his analogue card or giving a driving licence copy.

STEP 2

Amir opens his EUDIW by clicking on the deep link suggested on the car rental app or scans the QR code presented by the car rental officer.



STEP 3



Amir selects the data he needs to share with the car rental company to prove his right to drive and his identity.

STEP 4

Now, Amir can get into his car and enjoy his holiday in the Italian Alps.

STEP 5

Good to know.
The mobile driving licence generated by the EUDIW can also be used in case of a police check!

Use Case 5 Qualified Electronic Signatures (QES)

Overview of involved partners per Member States

14 countries participated: **AT, BE, CZ, DE, EE, EL, FR, FI, IT, LU, NL, PL, PT, UA**, with wallet issuers, QTSPs, and RPs.

Objectives and context

The pilots explored wallet-driven and QTSP-driven models for Qualified Electronic Signatures. They aimed to integrate secure, legally valid digital signing into wallet workflows under eIDAS 2.

Key results

UC5 proved both wallet-centric and QTSP-centric models feasible, supporting interoperability between wallets and QTSPs. However, legal uncertainties and evolving standards remain barriers to EU-wide adoption.

Technical recommendations

- Ensure secure, user-friendly signing flows.
- Provide mobile-ready open-source signature libraries.
- Standardise interfaces between wallets, QTSPs, and RPs.

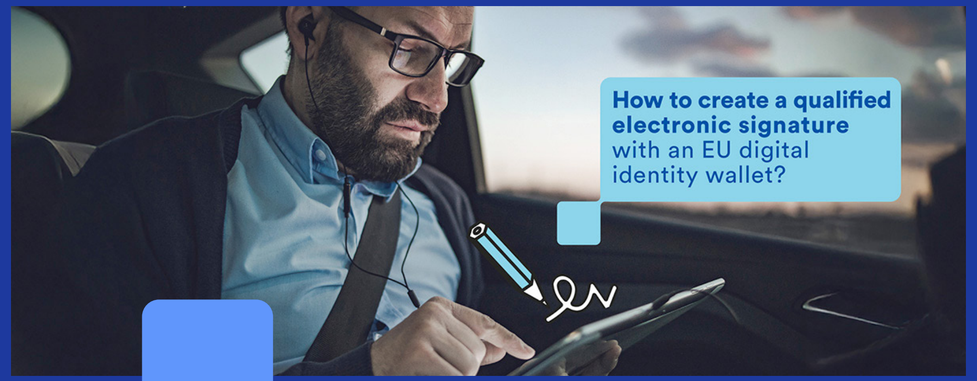
Legal recommendations

- Ensure harmonised Wallet interfaces for QES creation by Relying Parties.
- Amend the CSC requirements by Wallet-specific profiles once these are standardised.

Policy recommendations

- Mandate wallet-based QES acceptance by public authorities.
- Promote harmonised certification and conformance testing.
- Encourage adoption by both public and private RPs.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

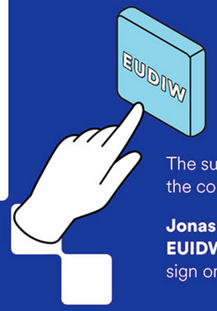


Jonas,
35 years old

Needs to sign
a contract with
a new service supplier.

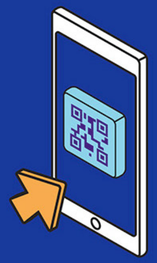
STEP 1

STEP 2



The supplier prepares
the contract to be signed.

Jonas chooses to use EUIDW to avoid print, sign on paper, and scan.



He **opens his wallet**
by using the QR code
or clicking the deep
link provided
by the supplier.

STEP 3

STEP 4

He inspects the contract and authorises his qualified electronic signature using his wallet.

STEP 5

And now,
Jonas can be sure the contract is officially signed!

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Use Case 6 ePrescription

Overview of involved partners per Member States

11 countries participated: **AT, CY, CZ, DE, FR, EL, HU, IT, PL, PT, UA**, with wallet issuers, health authorities, National Contact Points for eHealth, and an online pharmacy.

Objectives and context

UC6 tested wallet-based PID and Health ID credentials for cross-border pharmacy services. It piloted both proximity and remote transactions and integrated wallet-based flows with the MyHealth@EU identification services, supported by rulebooks for Health ID and ePrescription.

Key results

UC6 demonstrated the first cross-border online pharmacy transactions and patient identification for MyHealth@EU services using the wallet, and produced a pan-European Health ID rulebook, enabling harmonised health credential design. Proximity and remote flows were successfully tested with PID + Health ID.

Technical recommendations

- Ensure secure integration of health attestations in wallet flows.
- Provide reusable verifier tools for pharmacies and healthcare providers.
- Align wallet flows with MyHealth@EU infrastructure.

Legal recommendations

- Align the ePrescription/eDispensation workflow with the EUDI Wallet trust framework.
- Harmonise the health liability framework with the EUDI Wallet trust framework.
- Ensure EU-level adoption of Health ID and ePrescription attestations.

Policy recommendations

- Enable cross-border acceptance of ePrescriptions via wallets.
- Establish joint governance between identity and health authorities.
- Promote adoption of Health ID credentials across Member States.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Hélène,
62 years old

Needs to collect some medication, but she has not the paper prescription with her.

STEP 1

STEP 2

At the pharmacy, **she opens her EUDIW.**

The pharmacist scans the QR code provided by the doctor in Hélène's EUDIW.

STEP 3

STEP 4

And now, **Hélène can get her medication!**

Good to know.
The e-prescription via an EUDIW in another EU country is also possible.

The translation will be automatically made and the pharmacist will be able to find an equivalent to the required medication.

6. Diverse National Approaches

POTENTIAL revealed the diversity of national strategies for implementing the European Digital Identity Wallet. Member States differed in their governance models, levels of technical readiness, and adoption priorities. This diversity provides valuable lessons on balancing flexibility with EU-wide convergence.

Warsaw Interop Event (February 2025)

France

France actively coordinated the Consortium and contributed to several use cases, mobilising both **government agencies and major private actors**. ANTS, IN Groupe, and Docaposte worked alongside trust service providers like Namirial and financial institutions, including **BNP Paribas, La Banque Postale, BPCE, and Crédit Agricole**. This ensured that testing covered both government and high-impact private services, bridging regulatory and market perspectives.

In UC1 (government services) and UC2 (banking), France focused on **cross-border onboarding and authentication**, piloting PID and attestations such as proof of residence. Its involvement in UC4 (mobile driving licence) supported the exploration of wallet-based ISO-compliant credentials. This multi-sector engagement underlined France's strategy to make the EUDI Wallet relevant across domains from public administration to financial services.

France's approach demonstrates the value of **public–private collaboration and sectoral integration**. By involving leading banks and trust service providers, France tested the scalability of wallet adoption in sensitive domains, highlighting issues of liability, AML alignment, and user experience. This positioned the country as an example of how national ecosystems can **link regulatory leadership with market adoption** in preparation for the eIDAS 2 rollout.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Germany

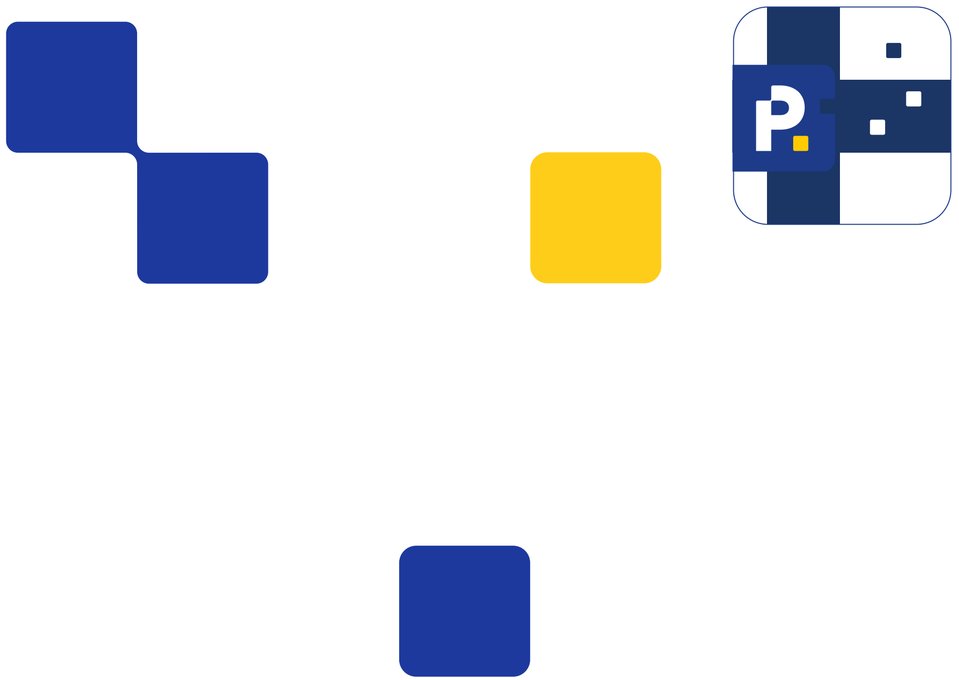
Germany piloted the Wallet across **telecom, mobility, e-government, e-signature, and health**, with the Federal Ministry of the Interior (BMI) coordinating national wallets and large private actors integrating as Relying Parties. In **telecom (UC3)**, **Deutsche Telekom, Vodafone, and Telefónica DE** tested wallet-based SIM registration and MSISDN issuing with multiple cross-border pairings (e.g., Austria, Czechia, Greece, Poland, Ukraine). German RPs deliberately connected **several national and private wallets** in parallel to stress-test interoperability and RP onboarding in a realistic market setup.

In **mDL (UC4)**, Germany combined **BMI/KBA** (issuer side) with private verifiers such as **Amadeus** and **LapID**, exercising both proximity and remote checks and hosting the July 2025 Berlin interop event. For **QES (UC5)**, Germany fielded multiple wallet implementations (e.g., Animo, Lissi, Ubique, wwWallet) and integrated with **D-Trust** as QTSP, validating both wallet-centric and QTSP-centric models and feeding concrete input on conformance, liability, and UX of signing flows.

Germany also enabled a first-of-a-kind **online-pharmacy** trajectory in **e-Prescription (UC6)**: with **Redcare Pharmacy** as RP and **Bundesdruckerei** providing PID issuance, pilots exercised **remote PID + Health ID** presentation where cross-border ePrescription services are emerging. Across use cases, Germany's contribution emphasised **multi-wallet interoperability, RP-grade onboarding**, and sector-specific scale requirements—producing actionable lessons for certification, test coverage, and production governance.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Finland



Finland positioned itself as an **early adopter**, piloting wallet use cases across **health, mobility, and government services**. In **mDL (UC4)**, Finland's **DVV and Traficom** acted as wallet and credential issuers, testing both **remote and proximity presentations** of driving licences, including revocation and combined PID+mDL flows. Finnish pilots were closely tied to ISO 18013 standards, ensuring alignment with international mDL specifications.

In **ePrescription (UC6)**, Finland leveraged its mature **MyHealth@EU integration** to test wallet-based **PID + Health ID credentials**. Cross-border transactions validated the feasibility of extending national ePrescription infrastructure to wallet ecosystems, with rulebook development laying the groundwork for harmonised health credentials.

Additionally, Finland contributed to **QES pilots (UC5)**, working with **Posti/QTSPs** to explore wallet-based signing in both user-driven and QTSP-driven flows. Overall, Finland demonstrated how a coordinated national strategy can extend wallets beyond eGovernment into **banking, healthcare, and mobility sectors**, with a strong emphasis on **cross-sector integration** and alignment with EU standards.

Italy

Italy played a **pioneering role** in several use cases, highlighting how wallets can support both public and private services. In **eGovernment (UC1)**, Italy's **Pago-PA and IPZS** tested wallet-based attestations for residence and company representation, demonstrating how wallets could streamline interactions between citizens, businesses, and public administrations.

In **mDL (UC4)**, Italy piloted both proximity and remote driving licence verification, with **IPZS** and regional partners such as the **Provincia autonoma di Trento**. These tests contributed to discussions on lifecycle management and alignment with the **4th Driving Licence Directive**. Italy also engaged in revocation testing, supporting the development of robust trust frameworks.

For **QES (UC5)**, Italian partners worked with QTSPs to trial **wallet-driven signing flows**, focusing on usability and compliance with eIDAS 2.0. Additionally, Italy was active in **ePrescription (UC6)**, integrating wallet-based flows with healthcare services and aligning with MyHealth@EU standards.

Overall, Italy's approach reflects its strategy as an **early adopter**, investing in **cross-sector integration** and ensuring that wallets can support a wide range of **government, mobility, and trust service applications**, while actively contributing to the development of European rulebooks.

Poland

Poland contributed actively across multiple use cases, focusing on **innovation and alignment with the Architecture and Reference Framework (ARF)**. In **eGovernment (UC1)**, Polish authorities and IT centres tested wallet-based attestations for identification and representation, ensuring that solutions complied with national legal and administrative frameworks.

In **banking (UC2)**, Poland's **COI and financial institutions** piloted wallet credentials such as PID, residence, and tax ID, linking them to **AML/KYC processes**. This helped explore how wallets could streamline customer onboarding while remaining compliant with financial regulations.

Polish partners were also heavily involved in **SIM registration (UC3)**, with **T-Mobile Poland** testing wallet-supported PID and MSISDN issuance in cross-border scenarios. These pilots underlined the need for **real-time verification** and scalability for telecom services.

Finally, in **mDL (UC4)** and **ePrescription (UC6)**, Poland tested interoperability with both mobility and health use cases, aligning its wallet solutions with **EU-level standards**. Overall, Poland's participation shows a **forward-looking approach**, experimenting with diverse wallet functions while ensuring close alignment with **ARF specifications** and practical regulatory needs.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Portugal

Portugal played a proactive role in the pilots, testing wallet use across **government, health, and trust services**. In **eGovernment (UC1)**, Portuguese authorities (AMA, INCM, IRN) explored the use of wallet-based attestations for identification, proof of residence, and legal representation, linking them to national registries and administrative services. These tests provided input for standardising attestation rulebooks at the EU level.

In **banking (UC2)**, Portugal trialled wallet credentials for **KYC/AML compliance**, including PID and tax ID attestations. The pilots highlighted both the potential for simplifying onboarding processes and the need for harmonised financial regulations across the EU.

Portugal was also an active participant in **QES (UC5)**, working with **national trust service providers** to test qualified electronic signatures directly in the wallet. This strengthened the link between wallet infrastructure and trust services under eIDAS 2.

Finally, Portugal contributed to **ePrescription (UC6)** through its national health authorities, validating **PID + Health ID credentials** in pharmacy scenarios. With this broad involvement, Portugal positioned itself as an **innovator**, testing wallet solutions closely aligned with the **ARF** and emphasising **multi-sector integration** to support real-life citizen services.

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

Ukraine

Ukraine contributed to the pilots by showcasing how its national **Diia wallet** could be integrated into the European framework. Diia is already widely used domestically for **eGovernment services**, identification, and access to public administration, giving Ukraine a unique starting point compared to most EU Member States.

In **UC1 (eGovernment)**, Ukraine tested wallet-based identification and authentication for cross-border services, aligning its Diia architecture with the **ARF** and exploring how national registries can interoperate at the EU level.

Ukraine also participated in **UC3 (SIM registration)**, working with Kyivstar and other partners to pilot **PID- and MSISDN-based flows**. This highlighted how mobile operators in non-EU countries can adopt the wallet ecosystem while meeting EU security and fraud-prevention standards.

In **UC4 (mDL)**, Ukraine joined cross-border pilots for mobile driving licences, validating interoperability of wallet-based mDL solutions in both proximity and remote settings.

Finally, in **UC6 (ePrescription)**, Ukraine tested wallet-based health credentials with its **National Contact Point for eHealth**, showing that the Diia model can extend to sensitive domains such as healthcare.

Through these contributions, Ukraine, as a country in the process of EU accession, demonstrated that non-EU countries can align with the EUDI Wallet ecosystem. This highlights opportunities for integration beyond EU borders while adding scale and diversity to the pilots

7. Conclusion and Next Steps

The POTENTIAL Large-Scale Pilot has demonstrated both the promise and the complexity of deploying a truly European digital identity solution. Across six diverse use cases, more than 1,000 cross-border transactions and hundreds of interoperability tests confirmed that the EUDI Wallet is technically feasible, while also exposing structural challenges that must be addressed.

Key achievements of POTENTIAL include building a functioning cross-border testing infrastructure, developing reusable attestations, validating wallet use in sensitive sectors such as health and banking, and generating invaluable user feedback. These contributions and recommendations provided to the European Commission will impact the further development of the Architecture and Reference Framework (ARF), the Reference Implementation (RI), and future Implementing Acts under eIDAS 2.0.

Vilnius Interop Event (May 2025)

UC4 Interoperability Testing Event Berlin (July 2025)

Looking ahead to 2026–2027, when Member States are required to roll out national wallets, the lessons of POTENTIAL provide a roadmap for success:

- Accelerate alignment with new versions of ARF and eIDAS, implementing secondary Acts to avoid divergent solutions.
- Establish strong national governance structures complemented by EU-level coordination forums.
- Mandate interoperability testing through a European conformance environment.
- Prioritise user-centric design, accessibility, and trust-building communication campaigns and forums.
- Ensure private sector integration from the outset, particularly in banking, telecoms, and health.

The transition from pilots to production will present challenges, but it is achievable if Europe acts collectively. POTENTIAL has laid the groundwork: the next step is for Member States, the European Commission, and industry stakeholders to build on this foundation and deliver wallets that are secure, interoperable, and trusted by all citizens across the EU.

8. Annexes

Board of Beneficiaries Paris (July 2023)

Glossary:

- **EUDI Wallet (European Digital Identity Wallet)** – A personal digital wallet that allows EU citizens, residents, and businesses to securely store and use identity data and electronic attestations across Member States.
- **ARF (Architecture and Reference Framework)** – The common technical and organisational framework defined by the European Commission to ensure interoperability of European Digital Identity Wallets.
- **QES (Qualified Electronic Signature)** – An advanced electronic signature that is created by a qualified electronic signature creation device and based on a qualified certificate, providing the highest level of legal assurance under eIDAS.
- **Secure Element** – A tamper-resistant hardware or software component that securely stores sensitive data and executes cryptographic operations in digital identity and trust services.
- **RP (Relying Party)** – An entity (such as a service provider, authority, or business) that relies on an electronic identification, signature, or attestation issued through the EUDI Wallet to provide services or verify identity.
- **QEAA (Qualified Electronic Attestation of Attributes)** – An attestation issued by a qualified trust service provider that confirms specific personal or organisational attributes with the highest level of assurance.
- **EAA (Electronic Attestation of Attributes)** – An electronic statement that confirms specific attributes (e.g., age, license, professional role) of a natural or legal person.
- **mDL (Mobile Driving Licence)** – A digital representation of a driving licence stored on a mobile device, developed according to ISO 18013 standards.

List of Standards

- **eIDAS 2.0** – The revised Regulation (EU) No 910/2014, establishing the European Digital Identity framework and introducing the European Digital Identity Wallet.
- **Implementing Acts** – Legally binding EU instruments adopted by the European Commission to specify technical details, standards, and procedures necessary for the uniform implementation of eIDAS 2.0.
- **ISO 18013-5/7** – International Organization for Standardization (ISO) standards defining interoperability and security requirements for mobile driving licences (mDLs) and their presentation.
- **OID4VP** – OpenID for Verifiable Presentations, a protocol enabling secure and privacy-preserving sharing of verifiable credentials based on open identity standards.

List of Legal Acts

- **European Digital Identity Regulation**
  Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183
- **Implementing Legal Acts (Regulations):**

List of Legal Acts

Adopted

1. Integrity and core functionalities

This Implementing Act, based on Article 5a(23) of the European Digital Identity Regulation, provides the necessary provisions to ensure that Member States set up European Digital Identity Wallets that are interoperable and effectively support their adoption: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202402979&qid=1733300667869

2. Certification

This Implementing Act, based on Article 5c(6) of the European Digital Identity Regulation, establishes the requirements for certifying the conformity of European Digital Identity Wallets and sets out the obligations for national certification schemes: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202402981&qid=1733300667869

3. Cross-border identity matching

This Implementing Act, based on Article 11a(3) of the European Digital Identity Regulation, sets out the provisions necessary for Member States to ensure correct identity matching in cross-border authentications: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500846

4. Protocols and interfaces to be supported

This Implementing Act, based on Article 5a(23) of the European Digital Identity Regulation, lays down provisions for the proper implementation of protocols and interfaces, which are crucial for the effective operation of European Digital Identity Wallets. Common protocols and interfaces enable seamless data exchange between wallet units and relying parties: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202402982&qid=1733300667869

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

List of Legal Acts

5. Personal identification data and electronic attestations of attributes

his Implementing Act, based on Article 5a(23) of the European Digital Identity Regulation, ensures the smooth lifecycle management of both personal identification data and electronic attestations of attributes, including their issuance, verification, revocation, and suspension: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202402977&qid=1733300667869

6. Security breaches

This Implementing Act, based on Article 5e(5) of the European Digital Identity Regulation, defines how security breaches must be addressed and specifies when and how compromised wallets should be suspended: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500847

7. Trust Framework

This Implementing Act, based on Article 5a(23) of the European Digital Identity Regulation, establishes an electronic notification system for Member States, operated by the Commission: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202402980&qid=1733300667869

8. List of certified wallets

This Implementing Act, based on Article 5d(7) of the European Digital Identity Regulation, sets out rules for Member States to submit information on certified wallet solutions for inclusion in the machine-readable list of certified wallets, which will be published and maintained by the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500849

9. Registration of relying parties

This Implementing Act, based on Article 5b(11) of the European Digital Identity Regulation, sets out rules for the registration of wallet relying parties through national registers: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500848

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

List of Legal Acts

10. Identity and recipients of qualified certificates

This Implementing Act, based on Articles 45d(5), 45e(2), 45f(6) and 45f(7) of the European Digital Identity Regulation, provides the specifications for issuing Qualified Electronic Attestations of Attributes (QEAA) and Electronic Attestations of Attributes (EAA), including provisions on interoperability and revocation mechanisms: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501569

11. Peer review of electronic identification schemes

This Implementing Act, based on Articles 12(6) and 46e(7) of the European Digital Identity Regulation, sets out provisions on the procedural arrangements for peer reviews of electronic identification schemes notified by Member States to the Commission: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501568

12. Qualified trust service applications

This Implementing Act, based on Article 21(4) of the European Digital Identity Regulation, establishes the formats and procedures for notifying supervisory bodies of a trust service provider's intention to offer qualified trust services: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501572

13. Verification of electronic attestation of attributes

This Implementing Act, based on Articles 45d(5), 45e(2), 45f(6) and 45f(7) of the European Digital Identity Regulation, provides the specifications for issuing Qualified Electronic Attestations of Attributes (QEAA) and Electronic Attestations of Attributes (EAA), including provisions on interoperability and revocation mechanisms: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501569

14. Remote qualified creation devices

This Implementing Act, based on Articles 29a(2) and 39a of the European Digital Identity Regulation, establishes the reference standards for managing remote qualified electronic signature creation devices and qualified electronic seal creation devices as qualified trust services: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202501567

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

List of Legal Acts

Acts in finalization
(feedback closed):

15. Annual reports by supervisory bodies

This Implementing Act, based on Articles 46a(7) and 46b(7) of the European Digital Identity Regulation, sets out the formats and procedures for the annual reports of the designated supervisory bodies responsible for supervising European Digital Identity Wallets and trust services: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14536-European-Digital-Identity-Wallets-annual-reports-by-supervisory-bodies-implementing-act-_en

16. Qualified certificates

This Implementing Act, based on Articles 28(6) and 38(6) of the European Digital Identity Regulation, sets out the reference standards and requirements for qualified certificates for electronic signatures and qualified certificates for electronic seals: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14654-Electronic-signatures-and-seals-qualified-certificates-implementing-act-_en

17. Trusted Lists

This Implementing Act, based on Article 22(5) of the European Digital Identity Regulation, ensures the validation of the qualified status of trust service providers and the trust services they provide. This amending decision lays down technical specifications and formats relating to trusted lists, including a reference to a new version of the standard cited in Commission Implementing Decision (EU) 2015/1505, as well as specifications on the format of signatures or seals to be used by Member States when signing or sealing their national trusted lists: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14612-eIDAS-Regulation-trusted-lists-amendment-to-implementing-act-_en

18. Reference standards & Validation procedures

This Implementing Act, based on Articles 32(3), 40, 32a(3) and 40a of the European Digital Identity Regulation, sets out a list of reference standards and, where necessary, establishes specifications and procedures for validating qualified electronic signatures and seals, as well as advanced electronic signatures and seals based on qualified certificates: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14651-Electronic-signatures-and-seals-reference-standards-validation-procedures-implementing-act-_en

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

List of Legal Acts

19. Qualified electronic registered delivery services

This Implementing Act, based on Article 44(2) of the European Digital Identity Regulation, sets out a list of reference standards and, where necessary, establishes specifications and procedures for the transmission and reception of data in the context of qualified electronic registered delivery services: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14650-Electronic-signatures-and-seals-qualified-electronic-registered-delivery-services-implementing-act-_en

20. Certified creation devices

This Implementing Act, based on Articles 31(3) and 39(3) of the European Digital Identity Regulation, sets out the formats and procedures for Member States to notify the Commission of certified qualified electronic signature and seal creation devices, as well as the cancellation of their certification, where applicable: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14653-Electronic-signatures-and-seals-certified-creation-devices-implementing-act-_en

21. Accreditation of conformity assessment bodies

This Implementing Act, based on Article 20(4) of the European Digital Identity Regulation, sets out rules to support the harmonised accreditation of conformity assessment bodies responsible for evaluating whether qualified trust service providers and the qualified trust services they provide comply with the applicable requirements. These rules cover the conformity assessment report and the conformity assessment schemes to be used when carrying out the assessment and providing the report: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14613-eIDAS-Regulation-accreditation-of-conformity-assessment-bodies-implementing-act-_en

22. Recognition of qualified validation services

This Implementing Act, based on Articles 33(2) and 40 of the European Digital Identity Regulation, sets out reference standards and, where necessary, establishes specifications and procedures for qualified validation services for qualified electronic signatures and seals: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14649-Electronic-signatures-and-seals-recognition-of-qualified-validation-services-implementing-act-_en

List of Legal Acts

23. Qualified preservation services

This Implementing Act based on Article 34(2) and 40 of the European Digital Identity Regulation sets out a list of reference standards and, where necessary, establishes specifications and procedures for the qualified preservation service for qualified electronic signatures and for qualified electronic seals: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14644-Electronic-signatures-and-seals-qualified-preservation-services-implementing-act-_en

24. Risk management procedures for non-qualified trust services providers

This Implementing Act, based on Article 19a(2) of the European Digital Identity Regulation, lays down requirements for non-qualified trust service providers. These requirements concern the management of legal, business, operational, and other direct or indirect risks related to the provision of non-qualified trust services: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14614-eIDAS-Regulation-risk-management-procedures-for-non-qualified-trust-service-providers-implementing-act-_en

25. Qualified electronic time stamps

This Implementing Act, based on Article 42(2) of the European Digital Identity Regulation, sets out reference standards and, where necessary, establishes specifications and procedures for binding date and time to data and for ensuring the accuracy of time sources with regard to qualified electronic time stamps: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14646-Electronic-signatures-and-seals-qualified-electronic-time-stamps-implementing-act-_en

List of Legal Acts

26. Qualified preservation services

This Implementing Act, based on Articles 34(2) and 40 of the European Digital Identity Regulation, sets out a list of reference standards and, where necessary, establishes specifications and procedures for qualified preservation services for qualified electronic signatures and seals: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14644-Electronic-signatures-and-seals-qualified-preservation-services-implementing-act-_en

27. Risk management procedures for non-qualified trust services providers

This Implementing Act, based on Article 19a(2) of the European Digital Identity Regulation, lays down requirements for non-qualified trust service providers. These requirements concern the management of legal, business, operational, and other direct or indirect risks related to the provision of non-qualified trust services: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14614-eIDAS-Regulation-risk-management-procedures-for-non-qualified-trust-service-providers-implementing-act-_en

28. Qualified certificates for website authentication

This Implementing Act, based on Article 45(2) of the European Digital Identity Regulation, sets out reference standards for qualified certificates for website authentication to ensure trust and transparency in online transactions: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14756-Qualified-certificates-for-website-authentication_en

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

List of Legal Acts

IA (drafts) open for public feedback (drafts released on 5th of September):

29. Qualified electronic archiving services

This Implementing Act, based on Article 45j(2) of the European Digital Identity Regulation, sets out reference standards and specifications for the qualified electronic archiving of electronic data and documents. These include rules on issuing reports to authorised relying parties: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14751-Qualified-electronic-archiving-services_en

30. Qualified electronic ledgers

This Implementing Act, based on Article 45l(3) of the European Digital Identity Regulation, ensures the integrity and accuracy of the chronological order of electronic data records. It sets out reference standards and specifications for qualified electronic ledgers, ensuring that data recorded in such ledgers is chronologically ordered, immutable, consistent, and reliable: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14752-Qualified-electronic-ledgers_en

31. Requirements on compliance and security for qualified trust service providers

This Implementing Act, based on Article 24(5) of the European Digital Identity Regulation, provides a list of reference standards, specifications, and procedures regarding the requirements for qualified trust service providers: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14754-Qualified-trust-service-providers-requirements-on-compliance-and-security_en

32. Formats of advanced electronic signatures and seals recognized by public sector bodies

This Implementing Act, based on Articles 27(5) and 37(5) of the European Digital Identity Regulation, provides reference formats for electronic signatures and seals, as well as reference methods for cases where alternative formats are used. Member States must recognise these formats and methods in order to process electronically signed or sealed documents and data: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14753-Advanced-electronic-signatures-and-seals-formats-to-be-recognised-by-public-sector-bodies_en

POTENTIAL:
FOR EUROPEAN
DIGITAL IDENTITY

References

POTENTIAL website

digital-identity-wallet.eu

European Commission's website for EUDIW

EU Digital Identity Wallet Home