Use Case Manual
eSignature

European Commission

EU Digital Identity Wallet

A Use Case Manual is a description of a specific use case for the EU Digital Identity Wallet. It includes an introduction to the use case and the user journey, the state of play of the use case development, as well as references to the relevant technical specifications and infrastructures, legislation, and governance structures.

The Use Case Manual is designed for the Wallet implementers, Member States and other stakeholders interested in the development of the Wallet and its use cases.

The Use Case Manual is not intended to contain full detailed technical specifications for the use case. However, where such specifications are available, the Use Case Manual contains pointers to them.

Description

A qualified electronic signature (QES) is an advanced electronic signature created by a qualified signature creation device (QSCD) and based on a qualified certificate for electronic signatures. It can be used in various situations: when signing an employment contract, when opening a bank account online, when declaring taxes or applying for a birth certificate... They hold the same legal standing as handwritten signatures.

The creation of qualified electronic signature by means of the Wallet can be achieved either by certified Wallet acting as QSCD and creating signatures locally, or through a remote QSCD which is managed by Qualified Trust Service Provider (QTSP). QTSPs get the qualified status by the national supervisory body and are reflected in corresponding national Trusted List.

POTENTIAL LSP piloted QES integration with remote signing services and Qualified Trust Service Provider (QTSP) functions.

User Journey(s)

Scenario 1
The wallet-driven qualified e-signature:

Simplified

1. User receives a rental contract (e.g., via email) and uploads it into his or hers EUDI Wallet.
2. Wallet displays the contract and its details for review and prompts user to sign with his or hers PIN/biometrics.
3. Wallet connects to a secure Trust Provider who verifies users' identity and officially seals the document on his behalf.
4. The contract is now legally signed and it can be sent back to landlord.

Detailed flow

1. Landlord prepares the PDF contract, signs it and sends it to user via email or instant messaging.
2. User opens EUDI Wallet (and authenticates using PIN/biometrics).
3. PDF into the wallet application signing feature.
4. Wallet displays the PDF contract (or opens it in a different app).

5. User reviews the document/data and instructs the wallet to sign the document.
6. Optional: User selects the signing service (if different than default or if enrolled in more than one service).
7. EUDI Wallet calculates the hash and sends it to the qualified trust service provider (QTSP) who is managing the qualified signature creation device on behalf of the user.
8. The QTSP requests the EUDI wallet to approve signing the document on behalf of the user.
9. The EUDI Wallet notifies the user of the pending approval request.
10. The user verifies the details of the transaction, and approves to sign.
11. The user authenticates using biometric or PIN and the Wallet creates a presentation to the QTSP e.g. presenting PID.
12. The QTSP verifies user approval, uses the user's keys to sign the document.
13. The QTSP returns to the wallet's signing application the signed document.
14. The PDF contract is now signed by both parties.
15. The user sends a copy of the signed document back to the landlord so that both of them have it.

Scenario 2

Relying Party driven application of e-signature - Signing via web portal

Simplified

1. User visits energy service provider web portal, signs up for service, goes through onboarding process and in the end reaches a contract signing step.
2. The portal displays the contract for review and, at the signature step, offers its Qualified Trust Service Provider (QTSP) for signature creation ("Sign with DocuSign").
3. User reviews the contract and scans the QR code to initiate a signature using PIN or biometrics.
4. Wallet sends cryptographic proof to secured Trust Provider, who signs and seals the document and sends it back to the Service Provider's system.
5. Web portal confirms that the contract is signed and the service is active.

Detailed flow

1. User visits energy service provider's who acts as Relying Party (RP) web portal and signs up for service.
2. Supplier prepares and provides a contract to be signed.
3. The portal displays the contract for review and, at the signature step, offers its QTSP provider for signature creation ("Sign with DocuSign").
4. User reviews the contract and proceeds.
5. The RP sends to the QTSP the hash of the data and informs the QTSP of who is the intended signatory.
6. The QTSP then contacts the user's wallet to confirm user approval (either directly or by redirecting the user to a QTSP website where a QR code (or link) is presented to initiate the signing session).
7. The user opens the Wallet, reviews the identity of the requesting party.
8. User approves signing using their EUDI wallet (e.g. present PID to signing service provider).
9. The QTSP verifies user approval, uses the user's keys to sign the document.
10. The QTSP returns the returns the signed document to the RP's system.
11. RP builds the whole signature and finalizes creation of the signed document.
12. The web portal confirms to the user that the service agreement has been signed by both the user and the energy service provider and the user has been signed up for service.

Use case impact

Benefits

End-user/citizen value

The integration of Qualified Electronic Signature (QES) capabilities within the European Digital Identity (EUDI) Wallet offers substantial value to end users and citizens by enhancing both convenience and accessibility. Individuals can sign official documents securely from any location and at any time, without the need for additional hardware, software, or complex onboarding procedures. Once enrolled, citizens benefit from cost-free QES generation, thereby eliminating expenses typically incurred through third-party signature services. The legal equivalence of QES to handwritten signatures across all EU member states ensures a high degree of legal certainty, fostering trust in fully digital administrative and commercial transactions. Moreover, the use of strong authentication protocols and trusted certificates mitigates risks related to fraud, identity theft, and signature repudiation. By removing the need for printing, scanning, mailing, or in-person appearances, the system significantly accelerates process completion, thereby increasing efficiency for both citizens and service providers.

Value for service providers

For service providers, the deployment of Qualified Electronic Signature (QES) functionality through the European Digital Identity (EUDI) Wallet delivers significant operational and strategic benefits. Process automation enables the seamless digital execution of contracts, customer onboarding, and approval workflows across sectors such as banking, human resources, legal services, and telecommunications, thereby reducing cycle times and administrative burdens. By minimizing reliance on printing, postage,

physical storage, and manual document handling, organisations can achieve leaner workflows and lower operational costs. The streamlined, intuitive signing experience not only enhances customer satisfaction but also fosters trust by reducing transactional friction. Full compliance with the EU Digital Identity Framework Regulation ensures that QES executed via the EUDI Wallet enjoys cross-border legal validity, mitigating complexity in multi-jurisdictional operations. Furthermore, integration with Qualified Trust Service Providers (QTSPs) and robust authentication mechanisms safeguards document authenticity and strengthens defences against fraud and forgery.

Value for public authorities
For public authorities, the integration of Qualified Electronic Signature (QES) capabilities into the European Digital Identity (EUDI) Wallet represents a key enabler of comprehensive digital transformation. It facilitates the delivery of fully online public services -ranging from tax declarations and permit applications to requests for civil status documents -while ensuring secure, authenticated, and non-repudiable exchanges between citizens and administrations. The system's inherent cross-border interoperability, aligned with the EU Digital Identity Framework 2.0, supports seamless administrative collaboration across EU member states and guarantees mutual recognition of electronically signed documents. By reducing reliance on paper-based processes, postal communication, and in-person service delivery, public authorities can achieve greater operational efficiency, lower costs, and allocate resources more effectively to high-value public services.

Economic value and potential market size

This section will be updated once operational wallets, and their business models emerge

Synergies with other use cases

Further benefits from the use of the wallet for eSignature can be achieved through synergy with the following use cases:

- *Online payment authorization:*
  Electronic signatures can authorize high-value or regulated transactions, meeting strong customer authentication (SCA) requirements.

- *Natural or legal person representation:*
  Electronic signatures can validate that someone is officially acting on behalf of an organization or another person.

- *Open a bank account:*
  Banks could use QES to sign contracts remotely with full legal validity.

- *Educational Credentials:*
  Issuance and verification of diplomas, certificates, or transcripts could be digitally signed to ensure authenticity.

- *Electronic prescription (eP):*
  A QES can confirm a prescription came from a licensed practitioner, preventing forgery.

Use case implementation

Existing implementations

The use case was piloted in the **POTENTIAL**, where the 5th use case was focusing on QES integration with remote signing services and Qualified Trust Service Provider (QTSP) functions.

The use case was piloted in the **NOBID** project (as part of the main pilot - onboarding to financial services by QES) by 4 Member States (Denmark, Latvia, Germany, Italy), as well as Iceland and Norway.

In **Estonia**, the Smart – ID app allows users to authenticate and perform qualified electronic signatures (QES) meeting U Digital Identity Framework Standards. Smart-ID Basic is also available in **Latvia** and **Lithuania** and can only be used for internet banking.

The ID Austria is an app-based e-ID platform which includes digital authentication and e-signature functionalities.

The Carta d'Identità Elettronica (CIE) is **Italy's** electronic ID card which enables citizens to perform advanced electronic signatures (AdES), including PAdES and CAdES formats, using NFC and either PIN or biometric verification.

The itsme app offers the convenience of a single onboarding, log-in and signature process for numerous different online services to citizens of **Belgium**. The app is certified for eIDAS and can be used to meet PSD2 and GDPR requirements.

IDMe.cy is **Cyprus**' newly introduced national electronic identity (part of the "Digital Citizen" platform), offering high-assurance authentication and legally equivalent electronic signatures to handwritten ones.

Gov.gr Wallet is the official application of the **Hellenic Republic** which allows citizens to sign digital documents quickly and securely through docs.gov.gr.

Portugal's ID.gov.pt mobile app is a digital wallet that allows citizens to store their ID cards and export digitally signed PDF certificates with a state-backed qualified digital signature.

Diia is **Ukraine**'s open-source government services app that broadly integrates digital documents, digital signatures, and secure document exchange.

Legislation

Article 22 of the EU Digital Identity Framework Regulation obliges Member States to publish information related to the qualified trust service providers (QTSP) for which they are responsible, together with information related to the qualified trust services provided by them. Trust Service Provider gets the Qualifies status by the national supervisory body, which decision is reflected and published in corresponding 'trusted lists'. Commission Implementing Decision (EU) 2015/1505 defines the technical specifications of these trusted lists.

Following Articles 27 and 37 of the EU Digital Identity Framework Regulation, Commission Implementing

Decision (EU) 2015/1506 specifies minimum formats of advanced electronic signatures and advanced seals to be r**ecognised by public sector bodies to ensure cross-border interoperability** of the online services offered by then.

Source

Implementing Regulation 2024/2981: Lays down rules for the application of Regulation (EU) No 910/2014 regarding the certification of European Digital Identity Wallets and ensures that wallets handle qualified certificates and signature creation mechanisms (like QSCDs or rQSCDs) in a trustworthy manner, resulting in legally binding e-signatures.

Implementing Regulation 2024/2979: It explicitly recognizes that wallets must be able to receive or manage qualified certificates tied to Qualified Electronic Signature Creation Devices (QSCDs) and run signature creation applications (either integrated, separate, or remote), thus enabling qualified electronic signatures.

Implementing Regulation 2025/1567: Provides rules and defines how remote qualified electronic signature creation devices (rQSCDs) must be managed and governed.

Technical specifications, software libraries and infrastructure

Data model, format and proof mechanisms
QSCD is not necessarily in the physical possession of the signatory, but it can also be remotely managed by QTSP. As per section 3.9 of Architecture Reference Framework (ARF), the creation of QES using EUDI Wallet can be achieved in several ways:

- either EUDI Wallet itself could be certified as QSCD, or,

- The Wallet may interface with remote Qualified Electronic Signature Creation Devices (rQSCDs) managed by Qualified Trust Service Providers (QTSPs) to issue signatures. These connections must conform to the Implementing Acts' reference standards for remote signature device management.

The eSignature data model includes:

- **Signed content and metadata**, such as:
  - Signatory identity and attributes
  - Signature type (AdES or QES)
  - Timestamp and timestamp method
  - Signature profile (e.g. PAdES, XAdES)
  - Certificate information, revocation status, and trust chain

Proof mechanisms vary by format.

Issuance
The Wallet may serve as a user interface to initiate signing, transmit data to the rQSCD, and retrieve signed results.

As part of the ecosystem, the use of common interfaces and protocols for provisioning qualified electronic signatures and seals will create a unified European market for QTSPs offering remote signature services.

Verification
Verification typically occurs within the Wallet or relying-party systems using standardized eSignature validation protocols integrated with EU Trusted Lists and certificate paths. These must support validation of AdES/QES signatures using established ETSI profiles like PAdES, XAdES, CAdES, or ASiC containers.

See an example of verification process flow for the remote QES.

Trust framework
Trust services are used alongside the eSignature to ensure validity, including:

- *Time stamping:*
  the date and time on an electronic document which proves that the document existed at a point-in-time and that it has not changed since then .

- *Electronic seal:*
  the electronic equivalent of a seal or stamp which is applied on a document to guarantee its origin and integrity.

- *Electronic delivery:*
  a service that, to a certain extent, is the equivalent in the digital world of registered mail in the physical world.

- *Legal admissibility of electronic documents*
  to ensure their authenticity and integrity .

- *Website authentication:*
  trusted information on a website (e.g. a certificate) which allows users to verify the authenticity of the website and its link to the entity/person owning the website .

Without certainty on the legal validity of all these related services, businesses and citizens will remain reluctant to use digital interactions as their natural way of interaction because they will be unsure of the issue of a possible dispute.

This is the intention behind the EU Digital Identity Framework Regulation on electronic identification and trust services for electronic transactions in the internal market.

The provisions applicable to trust services set by the EU Digital Identity Framework Regulation apply directly in all 27 EU countries.

European Commission

EU Digital Identity Wallet