Classification: Public

EWC D4.7

OPERATIONAL SIGNING SERVICES PROVIDING QES FOR ALL WALLETS

WP4 TASK 4.4

Author: INTESI GROUP

Contributors: INTESI GROUP, VALIDATED ID, SIGNICAT, INFOCERT, DIGIDENTITY

Day of submission: 18/07/2025

Contents

Co-funded by the European Union

Revisions

Version	Date	Author	Changes
v1.0	June 11, 2025	Viky Manaila, Intesi Group	Final version reviewed and agreed by contributors. Under review of Project Coordinators.

Co-funded by the European Union

Executive Summary

This document provides an overview of the signing services that are able to offer QES for all wallets. In particular, the document starts by introducing the topic and providing an overview. Next, it details what wallets and which PIDs where used for testing followed by describing the results.

In EWC we focused on implementing remote signing services, which is only one of the options for performing signing with a wallet. Other methods for signing have been described in D4.8 - Overview and rationale for QES[1], which was published and submitted in September 2023.

At this moment it is formally not possible to provide QES with the wallets, because some of the legal requirements for QES are not yet operational (e.g. certified EUDI Wallets are not available yet and the European List of Trusted Lists does not cover the EUDI Wallet Ecosystem). The technical and operational setup of the signing services covered in this document will be compliant once the EUDI Wallet Framework is fully operational.

The core contribution of this deliverable can be found in the annexes where the QES providers detail their implementation and tests performed. Furthermore, the providers share their proof of implementation within the annexes by illustrating screenshots of the user journey. They also provided videos of the functionality which will be shared with the evaluators.

To bolster the European digital identity infrastructure and accelerate its practical deployment, several key recommendations emerge:

Firstly, addressing the absence of INTERPOL database access for document verification is of utmost urgency. Securing this access is crucial for ensuring the integrity of identity documents used within the European framework. Without it, comprehensive verification is impossible, creating a potential vulnerability.

Secondly, ongoing optimisation of the user experience remains paramount. Focus should be directed towards improving mobile-first onboarding processes, enhancing the reliability and speed of NFC reading capabilities, and refining push-based consent mechanisms for digital signatures.

Finally, expanding real-world Qualified Electronic Signature (QES) integrations within high-impact sectors like finance, legal services, and public administration across Europe should be prioritised. This proactive approach will demonstrate the practical value and versatility of the European digital identity infrastructure, driving adoption and fostering trust.

[1] https://eudiwalletconsortium.org/wp-content/uploads/2024/11/EWC-D4.8-Overview-and-rationale-for-QES_v1.pdf

Co-funded by the European Union

List of abbreviations

Acronym	Explanation
(Q)EAA	(Qualified) Electronic Attestation of Attribute
EAA	Non-Qualified Electronic Attestation of Attribute
Pub-EAA	Public Body Electronic Attestation of Attribute
ACM	Access Control Mechanism
AES	Advanced Electronic Signature or Seal
ARF	Architecture and Reference Framework
CBOR	Concise Binary Object Representation
CIR	Commission Implementing Regulation
CSC	Cloud Signature Consortium
COSE	CBOR Object Signing and Encryption
DTC	Digital Travel Credential
EDIR	European Digital Identity Regulation
eID	electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
ETIAS	European Travel Information and Authorisation System
ETSI	European Telecommunications Standards Institute
EUDI	European Digital Identity
F2F	Face-to-Face
FAQ	Frequently Asked Questions
FAR	False Acceptance Rate
FRR	False Rejection Rate
IBAN	International Bank Account Number
ICAO	International Civil Aviation Organization
ISO	International Organization for Standardization
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
LSP	Large Scale Pilot
MRTD	Machine Readable Travel Documents

Co-funded by the European Union

Acronym	Explanation
NFC	Near Field Communication
PAD	Presentation Attack Detection
PAN	Primary Account Number
PID	Person Identification Data
QC	Qualified Certificate
QES	Qualified Electronic Signature or Seal
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
RFC	Request for Comments
RQES	Remote Qualified Electronic Signature
RQeSAC	Remote Qualified electronic Signature Access Credential
SD-JWT	Selective Disclosure for JWTs (JSON Web Tokens)
SOG-IS	Senior Officials Group - Information Systems Security
SSP	Signing Service Provider
T&Cs	Terms and Conditions
TSP	Trust Service Provider

Co-funded by the European Union

1. Introduction

The purpose of this document is to provide an overview of the different electronic signature implementations using the EUDI Wallet by the Qualified Trust Service Providers participating in EWC. These implementations are based on the Deliverable 4.8 – Overview and rationale for QES[2], which was published and submitted in September 2023. This deliverable outlines the development of server-based signing using both long-term and short-term certificates.

Since the remote QES services are called from the server side, the EUDI Wallet is only used for authentication and as activation means for the remote signing. Importantly, this design choice removes the necessity for any signing capabilities to be integrated directly into the EUDI Wallet. Consequently, this allowed for the pilot phase of the signing process to commence without the burden of extensive development or dependence on the EUDI Wallet Reference Implementation.

Additionally, all interfaces used are already standardized, and actors in EWC can provide all needed services with less extra development to handle the EUDI Wallet for authentication. This streamlining facilitates a more efficient integration of electronic signatures within the broader framework of digital transactions.

It is important to note that participants in EWC Task 4.4 have closely collaborated with ETSI and CSC, the main organizations responsible for developing standards for Qualified Electronic Signatures (QES) and remote QES. Additionally, informal connections have been established with three other Large Scale Pilots (LSPs): NOBID, POTENTIAL, and DC4EU, focusing on the same topics.

1.1 RFC-010 Document Signing on a Remote Signing Service Provider using Long-Term Certificates

To ensure interoperability with the various Wallet solutions available in EWC, participants in Task 4.4 developed a dedicated document, referred to as RFC-010[3], which outlines the procedures for using the EUDI Wallet to digitally sign a document using long-term certificates on a Remote Signing Service Provider. The architecture covered in this specification follows the process of remotely signing a document using long-term certificates, handled by a Remote QES (or AES) Service, as detailed in Deliverable 4.8.

The interactions with the EUDI Wallet involved in this approach for document signing are part of the core EWC RFC specifications (RFC 001 – Issue Verifiable Credential and RFC 002 – Present Verifiable Credentials Workflow). This means that the implementations will work with any EUDI Wallet in EWC that is conformant.

[2] https://eudiwalletconsortium.org/wp-content/uploads/2024/11/EWC-D4.8-Overview-and-rationale-for-QES_v1.pdf

[3] https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc010-long-term-certifice-qes-creation.md

Co-funded by the European Union

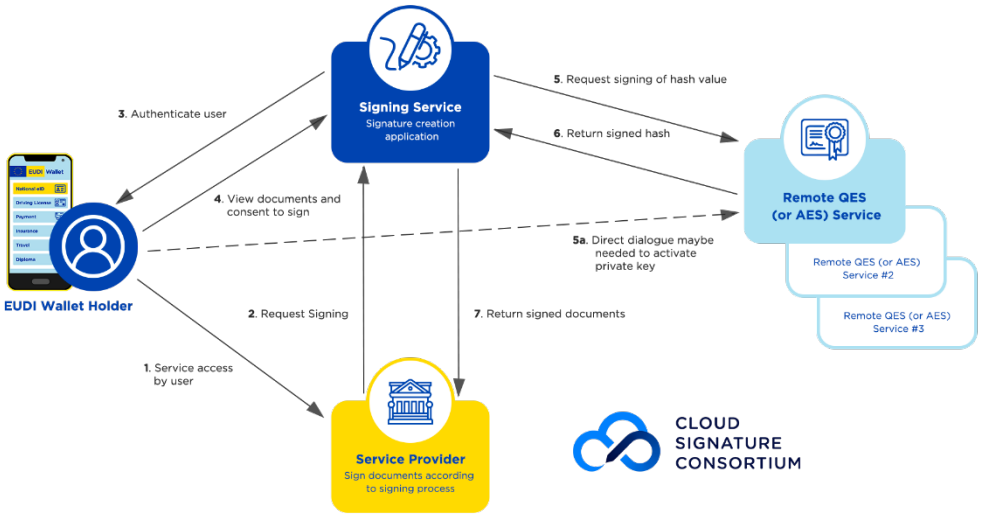


Figure 1: EWC Signing architecture using long-term certificate

The EWC repository, which contains all Request for Change (RFC) documents created to align the implementation of digital wallets across the consortium, is publicly available. This repository also allows all wallet providers to self-test and certify against the EWC Interoperability Test Bed. You can access the repository here:

https://github.com/EWC-consortium/eudi-wallet-rfcs/tree/main

1.2 Participating Beneficiaries

Five Qualified Trust Service Providers participating in the EWC Consortium, already delivering QES services, have implemented the signature generation with EUDI Wallet: Digidentity[4], Infocert[5], Intesi Group[6], Signicat[7] and Validated ID[8].

It is important to note that the initial commitment outlined in the Grant Agreement stipulated that seven operational Qualified Electronic Signature (QES) services would be available by the end of the project. However, three beneficiaries—Archipels, msg, and SIDN/IRMA—have left the consortium, and they were responsible for implementing QES generation through the wallet. As a result, the target of seven operational QES services can no longer be met. Nonetheless, the reduction in the number of operational QES services will have no overall impact, as the signatures were not utilised in the use cases that were piloted.

[4] https://www.digidentity.eu/
[5] https://www.infocert.it/
[6] https://www.intesigroup.com/en/
[7] https://www.signicat.com/
[8] https://www.validatedid.com/en

Co-funded by the European Union

2. Wallets used for testing

Under the Grant Agreement, beneficiaries involved in Large-Scale Pilots are initially obligated to prioritize testing and piloting with the EUDI Wallet Reference Implementation[9]. However, as the EWC implementation has progressed, a variety of alternative Wallet solutions that are fully compliant with the Architecture Reference Framework (ARF) have become available. This evolution necessitates the integration of signing capabilities for these newly available Wallets to ensure comprehensive testing and real-world applicability, in addition to the EUDI Wallet Reference Implementation. Specifically, the signing capabilities for QES generation have been successfully tested and verified with the following Wallets: Data Wallet from iGrant.io, Digidentity, ID Wallet from Validated ID, and the Thales Reference Implementation Wallet for the NOBID consortium. This expansion ensures a more diverse and representative testing environment, reflecting the broader ecosystem of EUDI-compliant solutions and fostering greater interoperability.

Wallet	Wallet Developer	Status	Comments
Data Wallet	iGrant	Pass	
Digidentity Wallet	Digidentity	Pass	
ID Wallet LSP	ValidatedID	Pass	
Reference Implementation Wallet	Netcompany – Intrasoft -Scytales	Pass	
NOBID Wallet	THALES	Pass	Tested as part of Cross-Consortium Testing (NOBID)

3. PIDs tested

The EWC participants have conducted comprehensive testing of Personal Identification Data (PID) integration for QES generation, demonstrating successful interoperability across various national and cross-border systems and wallet configurations. As part of this evaluation, the Finnish PID, already in use within the EWC pilot, served as a primary authentication method. Positive results across diverse national PIDs encompass the MojeID PID from Czech Republic, the UAegean Test PID from Greece, the Reference Implementation Test PID, the Norwegian PID and the Dutch PID. These were all confirmed as fully functional within the EWC framework. Notably, the Norwegian PID and Poste Italiane's PID were specifically tested as part of the cross-consortium testing with the NOBID wallet setup, underscoring the collaborative nature of the evaluation. Additionally, a PID from IPZS (Istituto Poligrafico e Zecca dello Stato) in Italy was tested with positive results.

These successful tests highlight the EWC's commitment to ensuring broad compatibility and interoperability of different wallet solutions, specifically in the context of QES creation. By validating the functionality of various national PID systems and collaborating with other consortia, EWC is actively contributing to the establishment of a robust and interconnected

[9] https://github.com/eu-digital-identity-wallet/.github/blob/main/profile/reference-implementation.md

Co-funded by the European Union

digital identity framework capable of supporting legally binding electronic signatures throughout Europe.

PID	Country	Status	Comments
MojeID PID	CZ	Pass	
UAegean Test PID	FI	Pass	
Reference Implementation Test PID	N/A	Pass	
Dutch PID	NL	Pass	
Norwegian PID	NO	Pass	Tested as part of Cross-Consortium Testing (NOBID)
Poste PID	IT	Pass	Tested as part of Cross-Consortium Testing (NOBID)
IPZS PID	IT	Pass	Tested as part of Cross-Consortium Testing (NOBID)

4. Results of the tests

The various implementations in EWC have successfully tested the signature of documents using the so-called "Relying Party centric model" described by the ARF 2.1 Annex 4.06 – Remote QES creating using EUDI Wallet for authentication and authorisation[10]. The testing scenarios included participants who already had long-term certificates issued, where these existing certificates were used for signing. Furthermore, the process of digital certificate issuance by the Qualified Trust Service Provider (QTSP) has been rigorously tested. This process relies on personal identification (PID) presentation and verification that occurs prior to the signing event, ensuring that only authorised individuals can access and sign documents securely.

The tests have been conducted during March – June 2025.

5. Conclusion and recommendations

EWC has successfully implemented and tested the capabilities of Qualified Electronic Signatures (QES) by utilizing EU Digital Identity (EUDI) Wallets. This testing focused on straightforward scenarios that involve a single signer, one document, and a remote signing process conducted by the Relying Party, also known as the Signing Service Provider. By employing the EUDI Wallet as a means of electronic identification for users, which provides a high Level of Assurance, the process of onboarding users for QES generation has been significantly streamlined. This innovative approach not only enhances security but also improves user experience by making it easier and more efficient to access electronic signing services.

[10] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/annexes/annex-4/annex-4.06-Remote-qes-creating-a-signature-eudi-wallet-used-for-authentication-authorisation.pdf

Co-funded by the European Union

Based on these experiences we are confident that any EUDI Wallet that is aligned to ARF 2.1 will be able to support this method for document signing and QES.

Since most of the beneficiaries involved in this task will be participating in the WE BUILD consortium, it is advisable to expand on existing achievements by developing more complex and diverse signing scenarios. These include situations with multiple signers for a single document, wallet-centric signature generation, and the implementation of (Q)EAA verification at the time of signing. The latter is especially crucial in a business context, as signing a contract or agreement often requires additional documentation, such as verifying company incorporation, power of attorney, or power of representation.

To bolster the European digital identity infrastructure and accelerate its practical deployment, several key recommendations emerge:

Firstly, addressing the absence of INTERPOL database access for document verification is of utmost urgency. Securing this access is crucial for ensuring the integrity of identity documents used within the European framework. Without it, comprehensive verification is impossible, creating a potential vulnerability.

Secondly, ongoing optimization of the user experience remains paramount. Focus should be directed towards improving mobile-first onboarding processes, enhancing the reliability and speed of NFC reading capabilities, and refining push-based consent mechanisms for digital signatures.

Finally, expanding real-world Qualified Electronic Signature (QES) integrations within high-impact sectors like finance, legal services, and public administration across Europe should be prioritized. This proactive approach will demonstrate the practical value and versatility of the European digital identity infrastructure, driving adoption and fostering trust.

Lastly, we invite the readers to consult the Annex where each implementing participant has provided specific recommendations.

Co-funded by the European Union

6. Annexes

6.1 Annex – Digidentity QES Integration

Operational Signing Services for EUDI Wallet

Name of the Provider: Digidentity B.V.

Qualified Electronic Signatures

Digidentity Solutions provides a fully operational Qualified Electronic Signature (QES) service integrated with the EU Digital Identity Wallet, enabling users to sign documents remotely using long-term qualified certificates. These certificates are issued under the authority of the “DDY Personal Qualified CA” intermediate certification authority, which itself is issued and certified by the “Digidentity SSCD Root CA””.

The signing process is executed through a Remote Qualified Electronic Signature (rQES) infrastructure conforming to the Cloud Signature Consortium (CSC) API specification. This infrastructure is uniquely built on a hybrid model: it utilizes a virtual smart-card in the Digidentity Wallet that connects the secure element of the user’s mobile phone with a Hardware Security Module (HSM) residing in Digidentity’s secure infrastructure. This architecture ensures end-to-end cryptographic protection and guarantees compliance with eIDAS2 standards.

The solution ensures high assurance, streamlined user experience, and regulatory alignment by binding the user’s Person Identification Data (PID) to each step in the signing workflow, including account creation, certificate issuance, and signature authorisation.

Flows/Diagrams

Digidentity’s Qualified Electronic Signature service supports multiple signing scenarios in partial alignment with the EUDI Wallet specifications outlined in EWC RFC010. The core flows include both user-initiated signing and Relying Party-initiated signing, each leveraging the EU Digital Identity Wallet for secure authentication and signature authorisation. In the user-initiated flow, the individual accesses the Digidentity signing portal, authenticates using their PID in SD-JWT format via the OID4VP protocol, and is guided through a streamlined process to issue a long-term qualified certificate if one is not yet available.

Once authenticated and authorised, the user uploads or selects a document for signing, and the system generates a cryptographic hash which is sent to Digidentity’s Signing Activation Module (SAM). The signature is then completed through a secure push notification to the Digidentity Wallet, where the user authorises the signing action. Upon user approval, the signing operation is performed at Digidentity’s back end using a remote Qualified Signature Creation Device (QSCD).

In the Relying Party-initiated flow, the signing request is triggered externally — for example by a financial institution — which uploads a document and redirects the user to the Digidentity signing interface. The user authenticates via their wallet and authorises the signature after

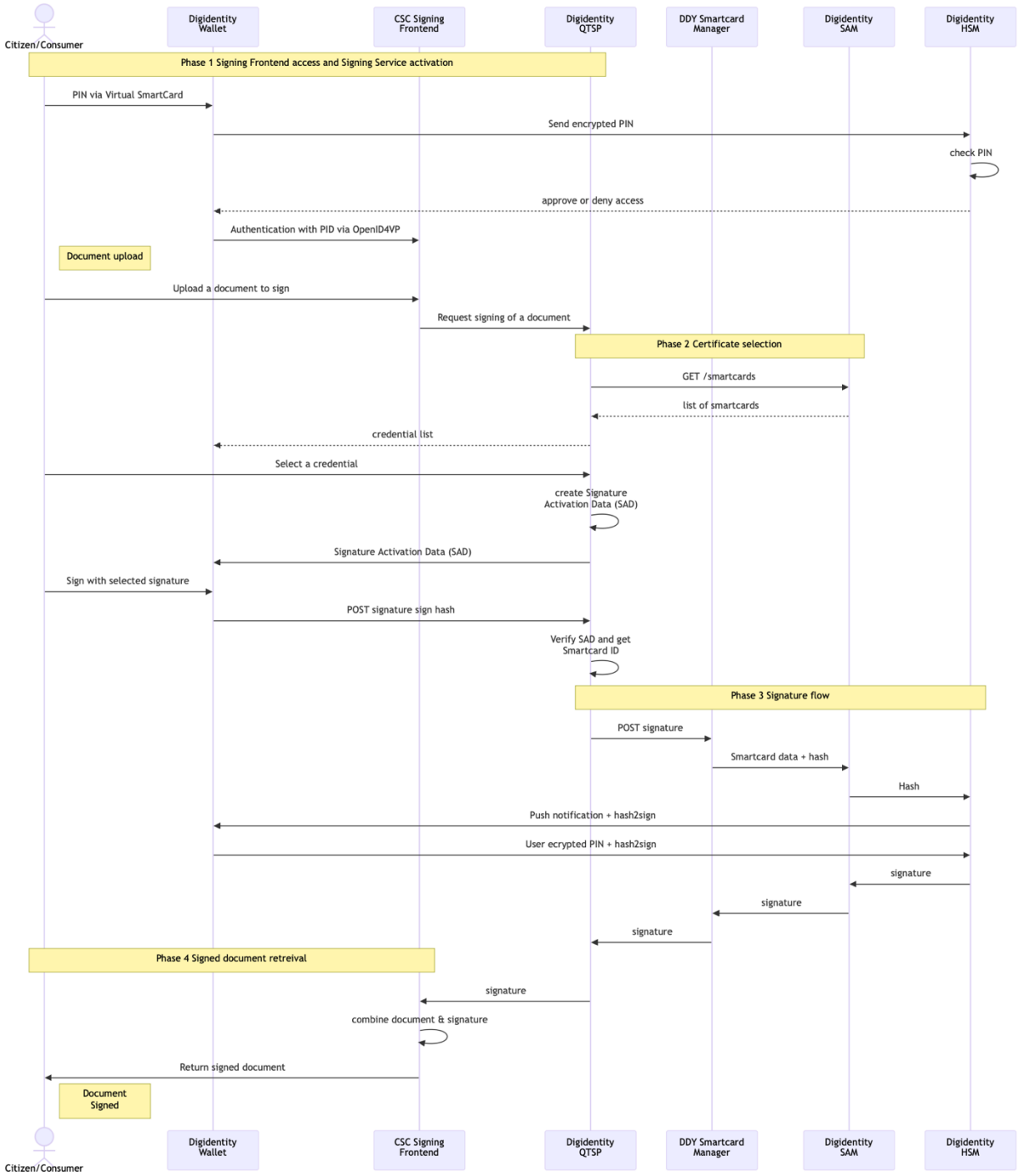
Co-funded by the European Union

reviewing the document. Each signature operation is cryptographically bound to the PID, ensuring integrity, non-repudiation, and cross-border legal recognition. The hybrid infrastructure — combining the mobile wallet, secure push-based consent, and Digidentity's SAM-HSM back end — guarantees both a seamless user experience and the highest level of trust and compliance.

Importantly, Digidentity's QES service is not limited to its own interface. It is fully interoperable with widely-used platforms such as Adobe Acrobat Sign and DocuSign, enabling users to apply qualified signatures directly within those environments using their EU Digital Identity Wallet. In all cases, the signature process maintains the same high-assurance workflow, with cryptographic binding to the user's PID and legal validity under eIDAS2.

See the Digidentity sequence diagram below.

Co-funded by the European Union



Co-funded by the European Union

Implementation

Digidentity's Qualified Electronic Signature (QES) solution is implemented using a modular, standards-based architecture that partially aligns with EWC RFC-010 for long-term certificate-based signing. The infrastructure combines Digidentity's remote identity proofing (eIDAS level High) and remote signing services with secure mobile wallet integration to deliver a seamless and compliant user experience.

At the core of the solution is Digidentity's remote Qualified Signature Creation Device (QSCD), which resides in a certified infrastructure environment backed by Hardware Security Modules (HSMs). Signing operations are authorised through the Signing Activation Module (SAM), which orchestrates the signature workflow by verifying user consent via secure push notifications sent to the Digidentity Wallet.

The solution leverages OpenID for Verifiable Presentations (OID4VP) to request and verify the user's Person Identification Data (PID) in SD-JWT format, establishing a strong link between identity and signature. The PID is used to bind a qualified certificate to the user's account during onboarding and later reused for secure, repeatable authorisations of signing actions.

Digidentity's architecture is compatible with the Cloud Signature Consortium (CSC) API, ensuring interoperability with third-party platforms such as Adobe Acrobat Signing and DocuSign. This allows relying parties to integrate Digidentity's remote QES capability into their existing document workflows without the need for custom development.

Authentication, consent management, and certificate lifecycle operations are all handled via Digidentity's secure back-end, which integrates with the EUDI Wallet for identity presentation and user authorisation. The signing infrastructure is horizontally scalable, cloud-native, and built with end-to-end security controls to support both individual and enterprise-level use cases.

Wallets used for testing

Digidentity has tested its Qualified Electronic Signature (QES) implementation only with the Digidentity wallet because lack of a level High authenticator in the other wallets.

Wallet	Developer / Provider	Status	Comments
Digidentity Wallet	Digidentity	Confirmed Working	Fully integrated push notification-based consent and QES authorisation.
iGrant Wallet	iGrant.io	Not confirmed	lack of a level High autheticator
Validated ID Wallet	Validated ID	Not confirmed	lack of a level High autheticator

Co-funded by the European Union

PIDs tested

Digidentity is authorised by the Dutch government during the EWC Large-Scale Pilot to issue Personal Identity Data (PID) based on identity data extracted from the NFC chip of passports and national identity cards. This process is compliant with eIDAS2 and offers high assurance by leveraging ICAO-compliant travel documents. Digidentity has validated identity data extraction from electronic identity documents issued by over 130 countries, ensuring broad international compatibility.

During all registration and signature workflows, Digidentity requested only the mandatory PID attributes, ensuring broad compatibility and privacy-conscious data minimisation.

Results of the tests

As part of the EWC Large-Scale Pilot, Digidentity executed extensive functional and interoperability testing to validate the full Qualified Electronic Signature (QES) workflow — from PID extraction and certificate issuance to signature authorisation and remote signing.

A central focus of our testing was the verification of Personal Identity Data (PID) extraction via NFC from electronic passports and national identity cards. Digidentity successfully tested and verified identity extraction and document qualification for signing from more than 130 countries, ensuring robust global coverage.

Digidentity has also validated the ability to create a PID based on the extraction of data from the NFC chip of the German Personalausweis.

These tests confirmed the ability to onboard users based on high-assurance identity documents, and also tested the ability to create Qualified Electronic Signatures based on existing Level of Assurance High (LoA High) electronic identities (eIDs), ensuring compliance with eIDAS2 requirements and cross-border trust.

Key results include:

- End-to-end successful signing of qualified PDF documents using Digidentity's own infrastructure and wallet.
- Verified creation of PID from over 130 countries' identity documents.
- Verified creation of PID from the German Personalsausweis eID.
- Signature metadata confirmed conformity with CSC specifications and eIDAS2 requirements.

All signed documents were validated to contain verifiable signature metadata, trusted timestamps, and a fully auditable identity binding based on the presented PID. The results demonstrate that Digidentity's solution offers strong technical readiness and regulatory alignment for real-world deployment in cross-border digital signing scenarios.

User Experience Testing

Unlike many pilot implementations, the Qualified Electronic Signature infrastructure integrated with the Digidentity Wallet is not experimental — it has been live and in production for over 10 years. This long-standing operational history means that the user interface, onboarding flows, and signature processes have already undergone continuous real-world user testing at scale. Millions of users across Europe have interacted with the system through a wide range of

Co-funded by the European Union

identity and signing use cases, from secure governmental services to high-value commercial transactions.

This production-grade maturity has provided Digidentity with invaluable insights into user expectations, usability issues, and authentication behaviour. As a result, the signing experience has been optimised to be frictionless, secure, and intuitive, reducing abandonment rates and ensuring high levels of user trust and satisfaction. This extensive field usage gives Digidentity a significant advantage over newly developed or theoretical implementations when it comes to readiness for mass deployment within the EUDI Wallet ecosystem.

Known Issues and Gaps

While Digidentity's infrastructure has proven robust in real-world usage, several systemic challenges were identified during the EWC Large-Scale Pilot that affect the reliability and completeness of high-assurance identity onboarding at a global scale.

One significant issue is that **not all trust anchors (root certificates) from the NFC chips of identity documents are available or published by the issuing countries**. This lack of a complete and trusted global repository for CSCA certificates (Country Signing Certification Authorities) limits the ability to fully verify the authenticity of certain travel and identity documents, despite their technical compatibility with ICAO standards.

Another critical limitation is **the absence of global access to the INTERPOL database of lost and stolen documents**. Without this connection, there is no authoritative way to validate whether an otherwise legitimate-seeming identity document has been reported as lost, stolen, or revoked. This undermines the integrity of digital onboarding workflows — particularly in remote or cross-border scenarios — and represents a significant gap in the global identity trust fabric.

These issues highlight that even with technically sound solutions, broader interoperability and security depend on international cooperation and infrastructure that extend beyond the scope of any single wallet or provider. Addressing these shortcomings is essential to achieving the full promise of secure, cross-border digital identity and signature services.

Demonstration of the implementation

1. NL Identity Proofing and PID Issuing - 2025 EU-NL-PID Issuing.mp4
2. DE Identity Proofing and PID Issuing - 2025 EU-DE-PID Issuing.mp4
3. QES Issuing - 2025 EU-QES Issuing.mp4
4. LT Signature via eSGN.com - 2025 EU-eSGN.mp4
5. Signature validation.com - 2025 EU-QES Validation.mp4

Demo portal

Digidentity Experience Portal (Pre-Prod)

Conclusion, recommendations and next steps

The Digidentity Qualified Electronic Signature (QES) service demonstrates a mature, scalable, and user-friendly solution that is already operational and trusted by millions. The system has proven its ability to create a Personal Identity Data (PID) via NFC from identity documents issued by over 130 countries, issue qualified certificates, and complete remote qualified signatures in compliance with eIDAS2 and CSC specifications. This includes real-world signing capabilities integrated into platforms such as Adobe Acrobat Signing and DocuSign.

Unlike many pilots, Digidentity enters the EUDI Wallet ecosystem with over a decade of production experience in remote signing and strong user identity binding — giving the solution a high level of readiness for mass deployment. Our infrastructure, including the Signing Activation Module (SAM), remote Qualified Signature Creation Device (QSCD), and mobile push consent workflow, ensures both security and usability at scale.

The pilot has also surfaced critical infrastructure and adoption challenges. One key issue is the lack of EUDI wallets equipped with Level of Assurance (LoA) High authenticators. Currently, the Digidentity Wallet is one of the few — if not the only — wallet that includes a high-assurance authenticator, enabling the creation of Qualified Electronic Signatures (QES) based directly on PID presented through the wallet. Until more wallets offer authenticators at LoA High, large-scale adoption of QES workflows through the EUDI Wallet will remain limited. This gap must be addressed at the ecosystem level to ensure broad, compliant rollout.

In addition, we identified systemic trust gaps such as the incomplete global publication of trust anchors (CSCA certificates) and the absence of access to the INTERPOL lost and stolen documents database. These prevent full verification of identity documents and should be treated as urgent priorities for the European digital identity infrastructure.

Next Steps

- Encourage harmonisation and adoption of LoA High authenticators in all EUDI Wallet implementations.
- Extend support for broader wallet compatibility and improve PID interoperability across the ecosystem.
- Collaborate with EU institutions and international bodies to mandate publication of CSCA trust anchors and enable access to Interpol’s lost/stolen document registries.
- Continue optimising the user journey, especially mobile-first onboarding, NFC reading, and push-based signing consent.
- Scale real-world QES integrations in finance, legal, and public sector applications across Europe.

Digidentity remains committed to advancing trust, usability, and interoperability across the European digital identity landscape, and to ensuring that qualified signing is accessible, secure, and future-proof.

Co-funded by the European Union

6.2 Annex – Infocert QES Integration

Operational Signing Services for EUDI Wallet

Name of the Provider: Tinexta Infocert

Qualified Electronic Signatures

Infocert implemented the QES with long-term certificates.

Flows/Diagrams

The objective of the implementation is to allow the quickest signing experience for a user that has already a long-term certificate available, avoiding the phase of QeSAC credential issuance, described in RFC-010. A second objective is to pilot the use of transaction data within the signature process, as mentioned in RFC-010, as a mean to bind the authorisation to the specific document to be signed references (hashes and URIs).

The user authenticates himself using his Infocert account credentials. Once authenticated, he has to choose one of the certificates that are bound to his account.

As soon as a document to be signed is uploaded or available, he accepts to sign it. Each signing certificate could have different authorisation mechanisms profiled, in order to guarantee a valid strong customer authentication. Two options are available to the user:

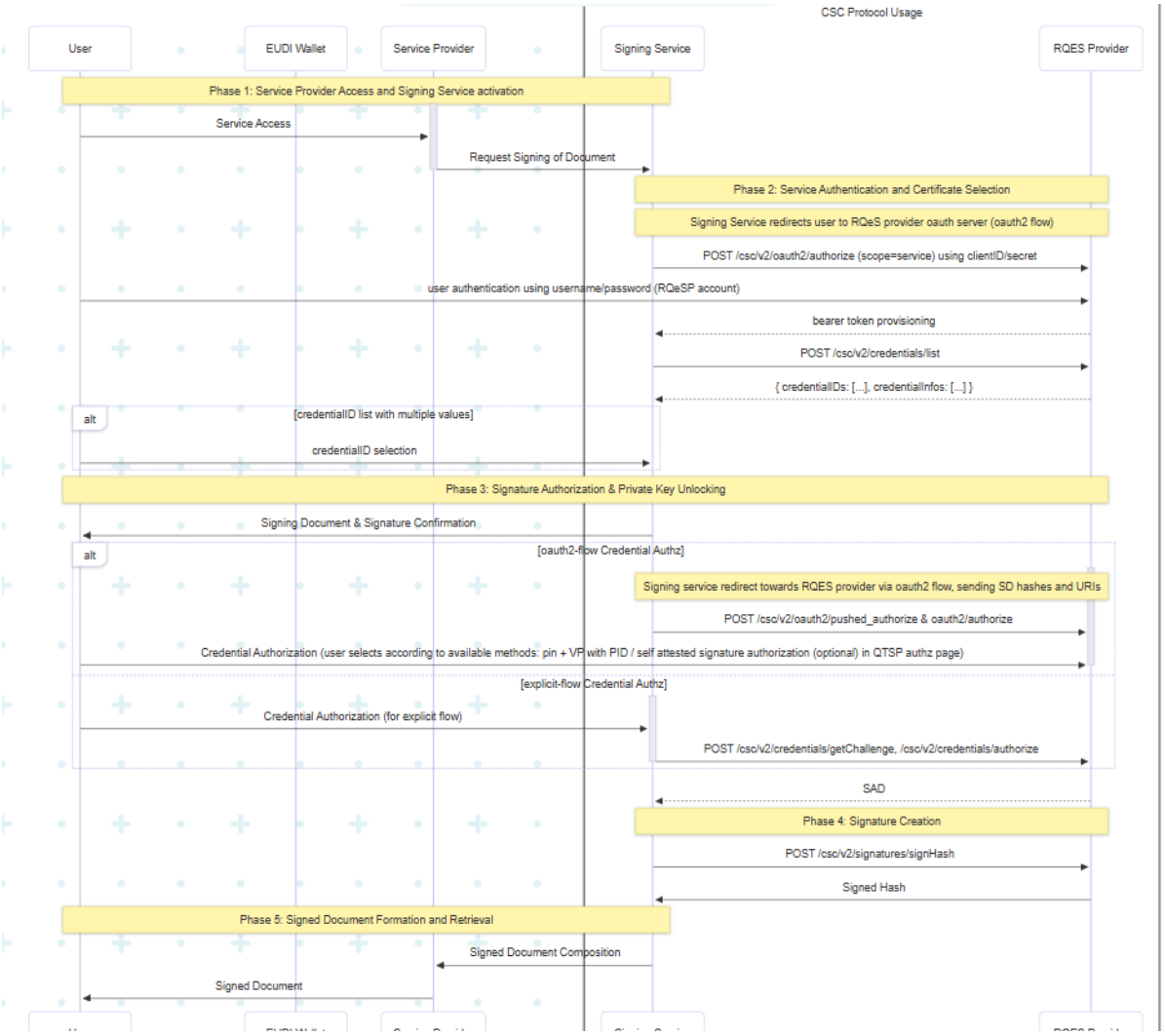
1. User could provide PIN and engage the SMS challenge process in order to collect a valid OTP that has to be filled in the form in order to authorise the signature
2. or User could provide the PIN of the certificate and select the “sign with wallet” option.

The first scenario describe the classic signature process; the second one includes a PID authentication with the wallet. A server side control ensures that the PID owner has the same name, surname and birthdate of the certificate’s owner. This proves the sole control of the authentication method.

In order to guarantee the inherence factor, the signing authorisation could include all information regarding the document (hashes and URIs) that are sent to the wallet in order to ensure linkability between the authorisation transaction and the document that has been previously viewed by the user in the Signing Service Application .

This is done using transaction data approval self-signed credential, aside with the PID request. This is technically supported only by OID4VP v23, that’s not yet supported in EWC ecosystem.

Co-funded by the European Union



Implementation

The implementation follows the specification of RFC-010.

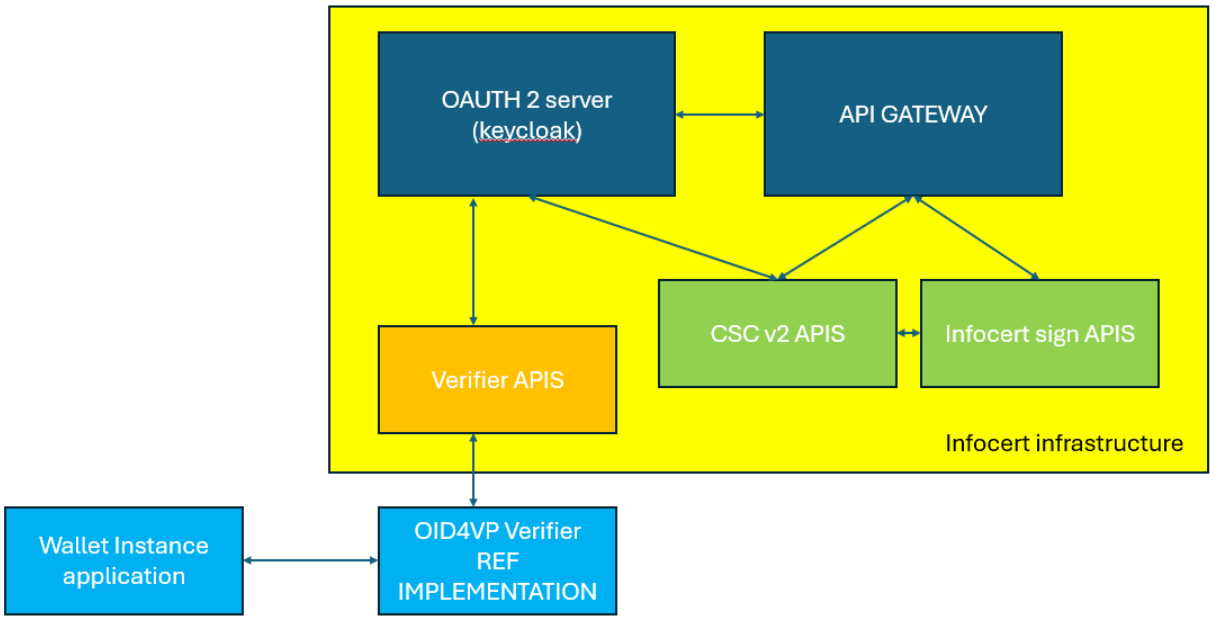
The Service Provider is represented by a web application (test application https://ewc-qtsp-sign.infocert-labs.eu/) that allows to upload a business document or offer a default one for testing purposes. The Signing Service would allow to access to different RQES providers: at this moment in the page it's possible to choose, but only one is available (Infocert).

RQES Provider exposes standard CSC APIs v2 (https://cloudsignatureconsortium.org/resources/download-api-specifications/). So the test web application behaves as Signing Service, authenticating itself to the RQES Provider API gateway using a specific clientID+secret.

Oauth2 authentication is managed using a keycloak platform.

The main element is the authorisation process that's engaged by the "/csc/v2/credentials/authorize": the testing verifier could be chosen by the test user in the webpage, and as soon as the user scans the QRcode and send the PID as VP response, the server checks the integrity of the token and compose the authorisation assertion with the token attached as evidence, and it is shared with the Infocert Sign API back end.

In the following diagram a quick description of the relevant architecture components is provided. Infocert sign service APIs have been wrapped in a new business API layer compliant with CSC v2 specifications. The verifier in engaged via rest API directly from the Oauth server, enabling vp token collection after wallet engagement.



Wallets used for testing

1. iGrant wallet
2. Validated ID wallet
3. Cross-consortium test has been made using NOBID wallet model A.

PIDs tested

The PID used for authentication is a Finnish PID (used in EWC pilot).

Cross-consortium and cross border tests: a test has been made using NOBID wallet configuration {PID provided by Poste IT and NOBID wallet}.

Results of the tests

Tests cases are successful, and this new authorisation method has been integrated in Infocert platform allowing a production deployment phase.

Demonstration of the implementation

1. long-term signature using iGrant wallet and Finnish PID (used in EWC pilot) (2025-05-28 LT using iGrant.mp4)
2. long-term signature using ValidatedID wallet and Finnish PID (used in EWC pilot) (2025-05-30 LT validatedID.mp4)
3. long-term signature using NOBID wallet (2025-05-26 16-37-13 LT NOBID.mp4)

Screenshots and demo-videos

Screenshots and demo-videos are available to the evaluators through the EWC document repository (NextCloud).

Co-funded by the European Union

Conclusion, recommendations and next steps

EUDIW has proven to be a powerful authentication tool, improving efficiency and usability for the user in signing processes. Comparing with traditional tools based on dynamic codes using different channels like SMS or specific QES provider apps, a wallet provides an intuitive and standard interface to interact with specific business transactions.

In this phase , PID authentication has proven to be easy to be used and reliable, so ensuring trust and improving user experience.

Next step is to include document to be signed references in the authorisation transaction managed in the wallet by the user. Transaction details that are bound to the authentication operation must be accessible to the user and directly linked to the PID or other verifiable credential presentation. This inherence factor will be crucial in the next future to avoid misuse of authorisation operations and user misinformation and errors, ensuring the customer that is seeing what he signs.

This goal will be reachable as soon as version 23 of protocol OID4VP, and technically has been included in RFC-010 for future reference.

Co-funded by the European Union

6.3 Annex – Intesi Group QES Integration

Operational Signing Services for EUDI Wallet

Name of the Provider: INTESI GROUP

Qualified Electronic Signatures

The Intesi Group Document Signing Service facilitates the generation of digital signatures utilising Long-Term Certificates. These certificates are issued under the authority of the “Intesi Group EU Qualified Electronic Signature CA Test” intermediate certification authority, which itself is issued and certified by the “Intesi Group Cloud Root CA Test” certification authority. The digital signatures are based on the SHA-256 with RSA encryption algorithm (OID: 1.2.840.113549.1.1.11).

The private signing key is securely stored within a Qualified Signature Creation Device (QSCD), ensuring compliance with eIDAS2 requirements for qualified electronic signatures. The signature operation, specifically, the signing of the hash, is executed via a Remote Qualified Electronic Signature (RQES) service that adheres to the Cloud Signature Consortium (CSC) API specification.

Flows/Diagrams

The Intesi Group Proof of Concept (PoC) Document Signing Service integrated with the EU Digital Identity Wallet supports multiple use cases. These include scenarios where a user initiates the signing of a document independently from the Wallet, as well as cases in which a Relying Party, such as a financial institution—requests the user to sign a document, e.g., a contractual agreement.

The service is fully compliant with the specification defined in EWC RFC-010, which outlines the standardised approach for long-term certificate-based Qualified Electronic Signature (QES) creation using the EU Digital Identity Wallet.

Use Case 1: The user uploads the document to be signed

The user navigates to the authentication page of the Document Signing Service, where they may either log in or register for an account if they do not already possess one.

During the registration process, the user is prompted to present their Person Identification Data (PID) in SD-JWT format via the OpenID for Verifiable Presentations (OID4VP) protocol. This step enables the service to retrieve essential attributes required for user registration.

Upon completing the registration form, a user account is created. A unique hash derived from the PID is then generated and linked to the user's account. Access to this account is restricted exclusively to the legitimate PID holder.

After registration, the user proceeds to log in. During the login process, the system requests the presentation of the user’s PID as a second factor for authentication, reinforcing the identity verification process.

If the user does not yet possess a signing certificate, the system prompts them to initiate the issuance process. On the certificate issuance interface, the user is again required to present their PID. This step ensures that the certificate request is both authenticated and intentional,

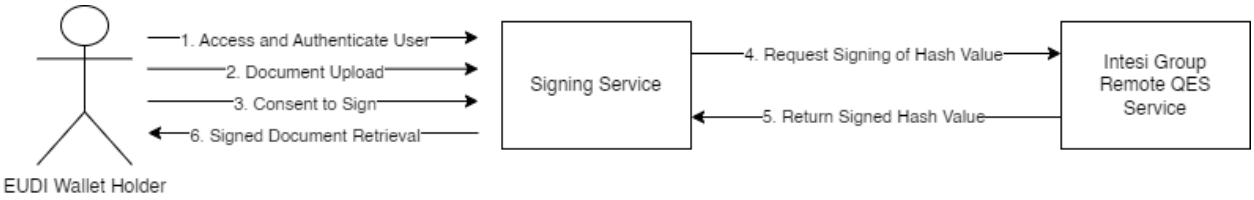
Co-funded by the European Union

confirming that it originates from the rightful account holder. Once verified, a qualified digital certificate is issued and becomes available for use.

The user may now upload the document to be signed in PDF format via a drag-and-drop interface. A preview of the uploaded document is made available for the user to review.

To authorise the digital signature, the user is prompted once more to present their PID. Following successful verification, the system computes a cryptographic hash of the document and transmits it to Intesi Group's Remote Qualified Electronic Signature (QES) Service.

Upon successful signing, the signed hash is retrieved and programmatically embedded into the PDF document, thereby producing a digitally signed document. The final signed document is made available for the user to download and use as needed.



Use Case 2: A Relying Party uploads the Document to be Signed

In this scenario, a Relying Party, represented by an example entity such as a bank, requests that a user sign a Terms and Conditions Contract. The Relying Party initiates the process by uploading the document directly to the Document Signing Service, eliminating the need for user interaction during the upload phase. The user is then redirected to the signing service to complete the signature process.

Upon redirection, the user is taken to the authentication page of the signing service, where they may either log in or create a new account. During registration, the user is prompted to present their Person Identification Data (PID) in SD-JWT format using the OpenID for Verifiable Presentations (OID4VP) protocol. This allows the service to prefill essential personal data for account creation.

Once the registration form is completed, the system creates a user account. A unique hash of the PID is generated and is bound to this account, ensuring that only the legitimate holder of the PID can access it. The user is then prompted to log in.

As part of the login process, the user is again asked to present their PID as a second factor of authentication, adding a layer of assurance to the identity verification process.

If the user does not yet possess a qualified digital certificate, the service prompts the user to initiate the certificate issuance process. During this process, the user is required to present their PID once more, ensuring that the request originates from the account holder and is submitted voluntarily. Upon successful verification, a signing certificate is issued and made available for use.

The user is then presented with the document that was previously uploaded by the Relying Party. After reviewing the document, the user is asked to present their PID once again to authorise the signature operation.

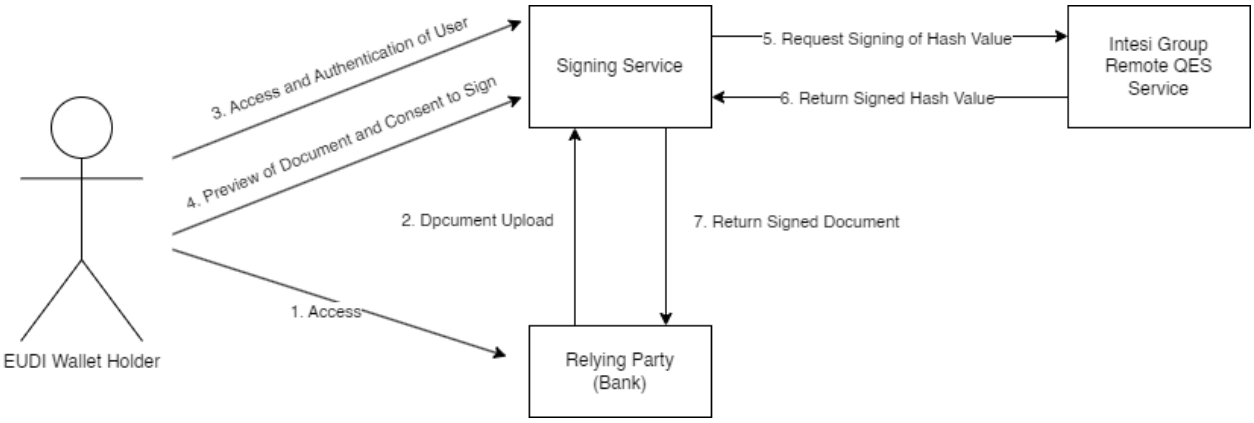
Co-funded by the European Union

Upon confirmation, the cryptographic hash of the document is generated and securely transmitted to Intesi Group's Remote Qualified Electronic Signature (QES) Service for signing.

Following successful remote signature creation, the signed hash is retrieved and embedded into the original document, resulting in a digitally signed PDF file.

The user is then provided with the option to download the signed document. In parallel, the Relying Party is able to retrieve the signed document for further processing and verification.

For this flow to be executed, Relying Parties must have followed the Integration Guide, provided by Intesi Group.



Implementation

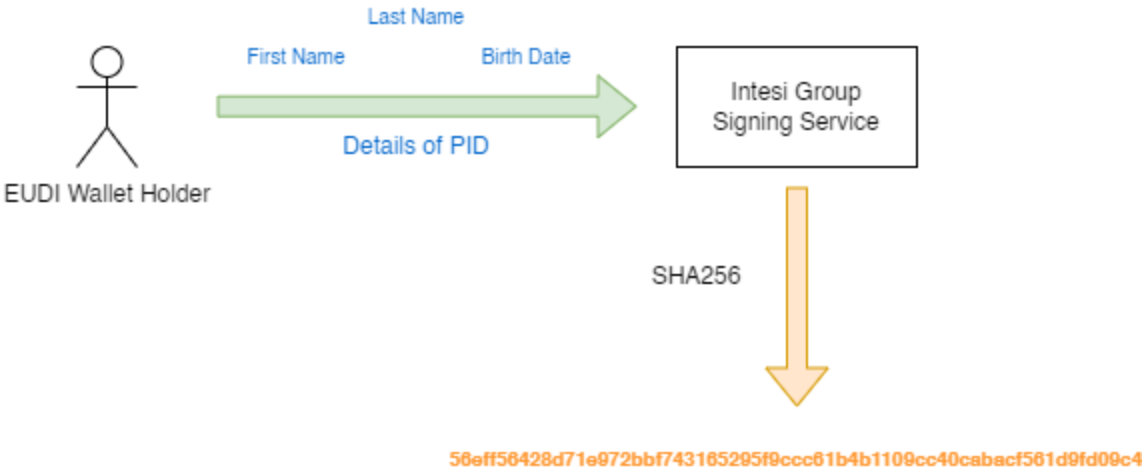
Usage of the EUDI Wallet as a means of Authentication/Authorisation

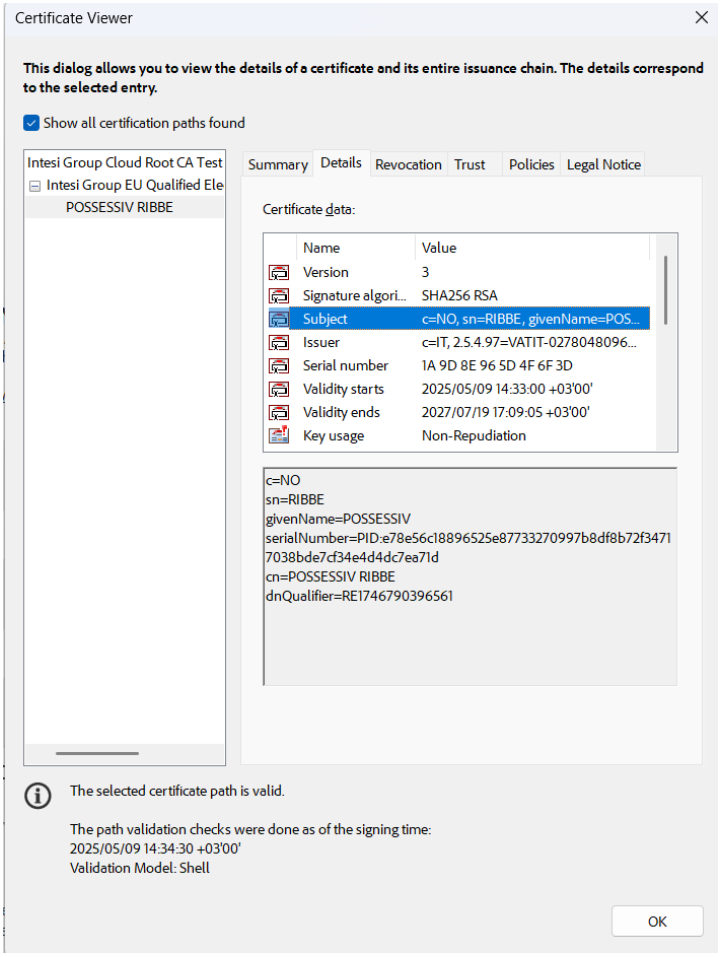
Throughout the entire document signing workflow, whether in Use Case 1 (user-initiated signing) or Use Case 2 (Relying Party-initiated signing), the EU Digital Identity Wallet serves as the primary mechanism for user authentication and authorisation of the signature.

During the registration process, the user's Person Identification Data (PID) is presented via the Wallet in SD-JWT format and is used to derive a unique, cryptographically secure hash. This hash is bound to the user's account and subsequently utilised in all critical security-sensitive operations, such as certificate issuance and signature authorisation. By leveraging the Wallet's secure storage and presentation capabilities, the system ensures that only the legitimate PID holder can access and operate the account.

This approach reinforces strong user authentication and ensures a high level of assurance, as required by the eIDAS2 Regulation for qualified electronic signatures.

Co-funded by the European Union





Usage of the Wallet as a means to improve User Experience

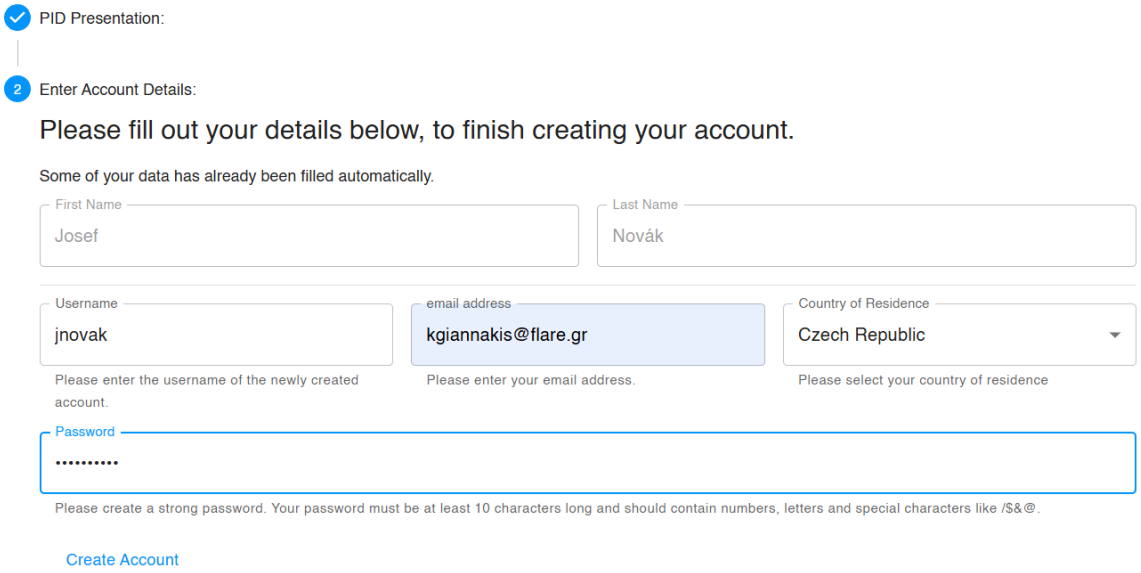
The integration of the EU Digital Identity Wallet significantly enhances the user experience across various stages of interaction with the Document Signing Service.

Prefilling of User Information during Registration

During the registration process, selected attributes from the user's Person Identification Data (PID), presented via the Wallet, are utilised to automatically prefill fields in the registration form. This reduces manual input, streamlines the onboarding process, and minimises the

Co-funded by the European Union

potential for data entry errors. As a result, the overall registration experience becomes more efficient and user-friendly, while maintaining high standards of data integrity and compliance.



Improved Authorisation flows

The use of the EU Digital Identity Wallet introduces a streamlined and secure approach to user authorisation by leveraging PID-based verification mechanisms. As previously described, the user's PID is hashed during registration and securely bound to their account. This hash is subsequently used to verify the user's identity during critical operations, ensuring that actions are only performed by the legitimate account holder.

This method significantly improves the flow of authorisation throughout the signing process. By using the presentation of the PID as a form of two-factor authentication (2FA), the system eliminates the need for less secure or more cumbersome channels, such as SMS or email-based verification codes. This not only enhances the security posture of the system but also simplifies the user experience.

The same mechanism is employed during signature confirmation, where PID presentation ensures that the request to sign a document is both authenticated and deliberate. This consistent application of secure and user-centric authorisation reinforces trust, compliance, and usability across the service.

Wallets used for testing

Wallet Tested	Wallet Developer	Status	Comments
Data Wallet	iGrant	Confirmed Working	
ID Wallet LSP	ValidatedID	Confirmed Working	
Reference Implementation Wallet	Netcompany – Intrasoft -Scytales	Confirmed Working	
NOBID Wallet	THALES	Confirmed Working	Tested as part of Cross-Consortium Testing (NOBID)

Co-funded by the European Union

PIDs tested

PID Tested	Country	Status	Comments
MojeID PID	CZ	Confirmed Working	
UAegean Test PID	FI	Confirmed Working	
Reference Implementation Test PID	N/A	Confirmed Working	
Norwegian PID	NO	Confirmed Working	Tested as part of Cross-Consortium Testing (NOBID)
Poste PID	IT	Confirmed Working	Tested as part of Cross-Consortium Testing (NOBID)
IPZS PID	IT	Confirmed Working	Tested as part of Cross-Consortium Testing (NOBID)

During Registration and subsequent presentations, only the mandatory PID attributes specified in CIR 2024/2977 are requested as to improve cross-border and cross-PID-Provider compatibility.

Results of the tests

Functional tests (internal)

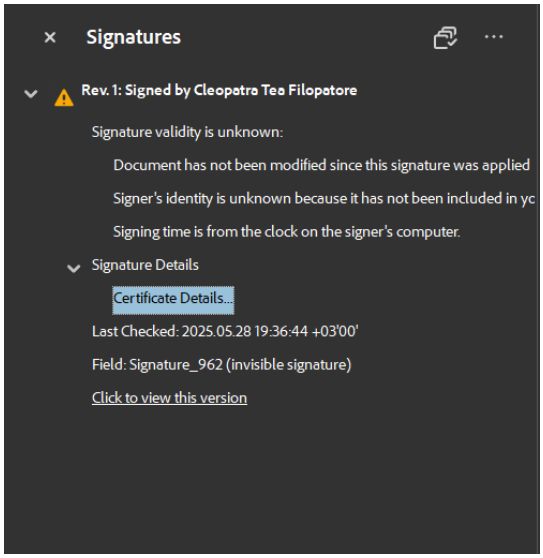
Intesi Group tested the implementations using the EUDI Wallet Reference Implementation, as well as various Wallets available within EWC. During the fourth week of May, functional testing was conducted within the framework of the NOBID consortium. These tests involved the use of the Intesi Group Document Signing Service and focused on validating the end-to-end signature workflows in a real-world scenario (applicable to Use-Case 2).

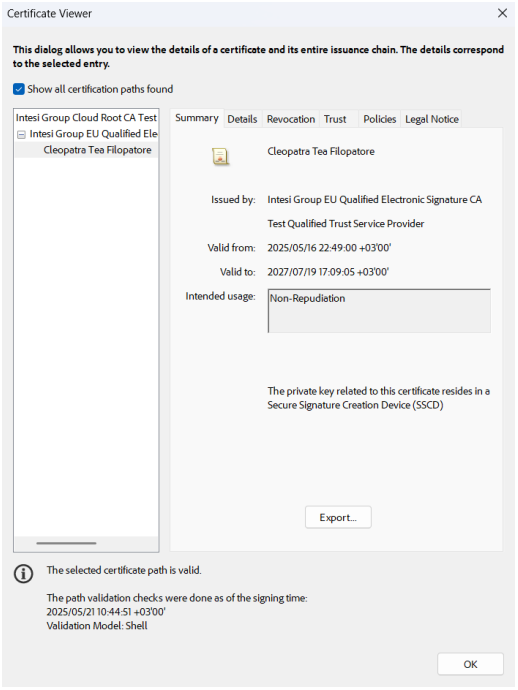
As a result of the testing activities, a total of 37 documents were successfully signed, demonstrating the operational integrity, interoperability, and usability of the signing service when integrated with the EU Digital Identity Wallet.

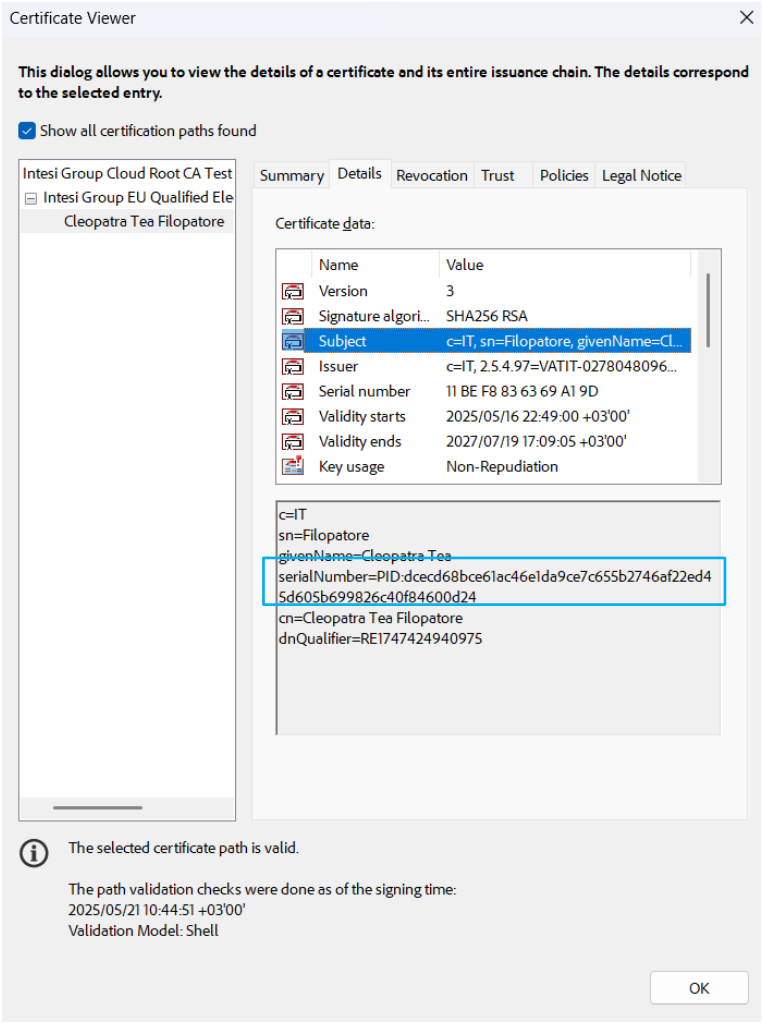
Screenshots detailing the signature metadata of selected signed documents are provided below as supporting evidence of successful execution. **It should be noted that in the certificate field Subject, the serial number contains the hash of the PID used as identity verification method for the certificate generation.**

Document 1:

Co-funded by the European Union

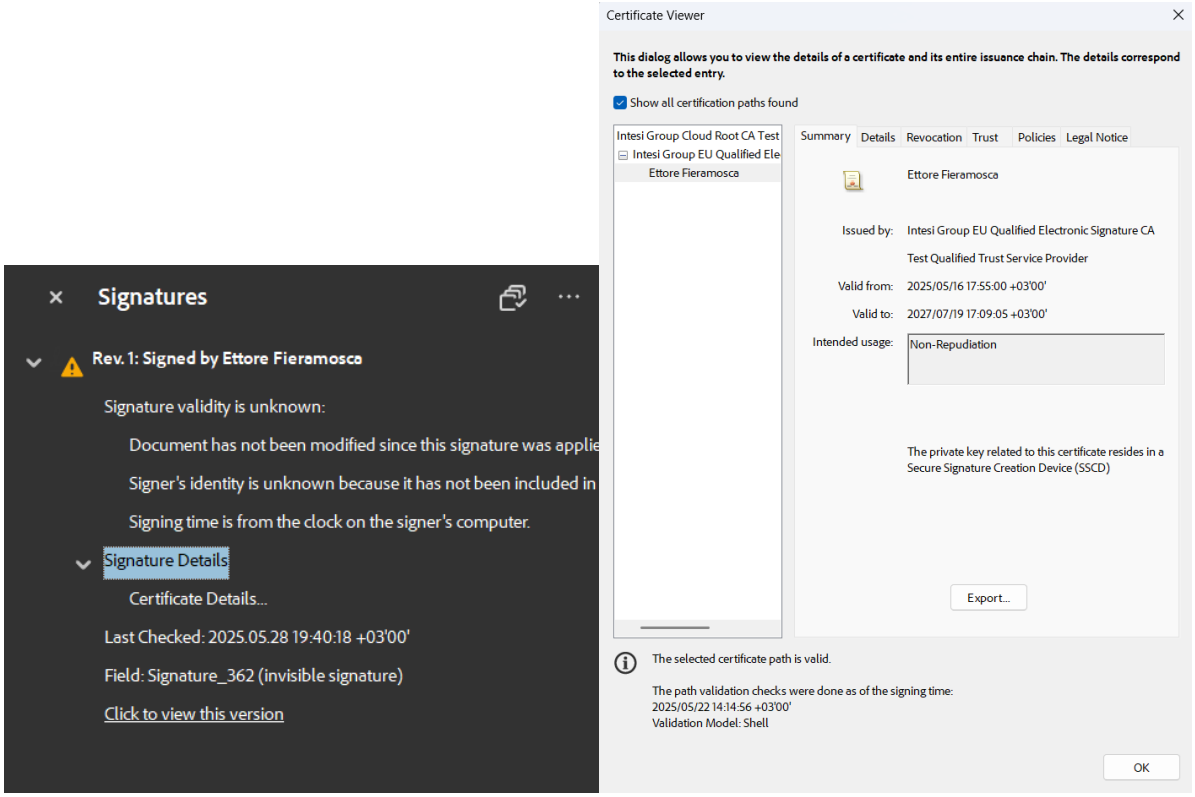


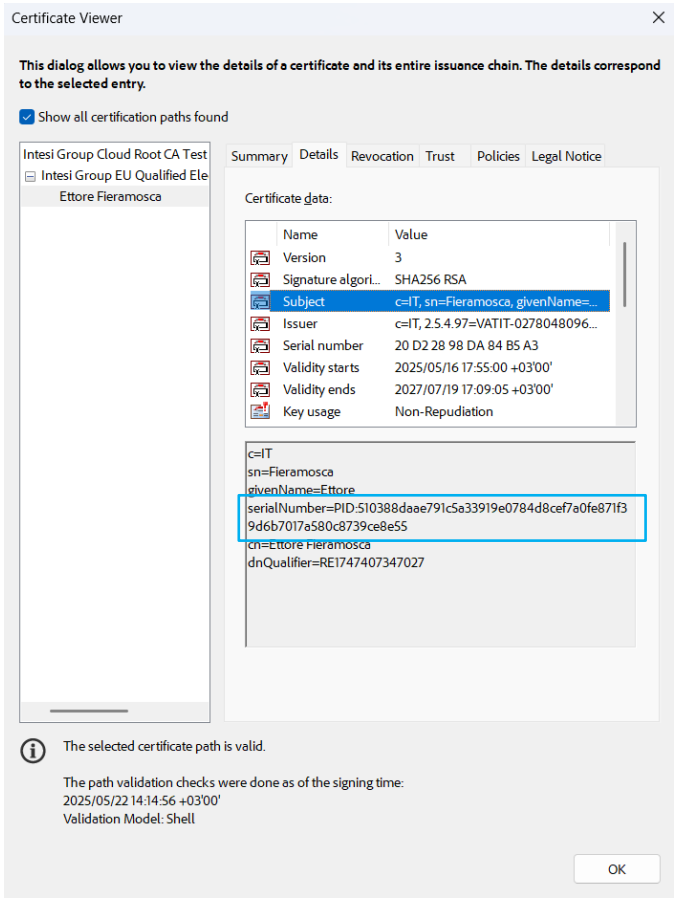




Document 2:

Co-funded by the European Union





Co-funded by the European Union

UAT - User experience

The Intesi Group Document Signing Service underwent comprehensive User Acceptance Testing (UAT), involving both internal developers from Intesi Group and sub-contractor Flare, as well as selected end-users participating in functional testing scenarios.

Throughout the development lifecycle, continuous feedback was collected regarding the platform's usability and workflow efficiency during the months of March and April 2025. Based on this feedback, it was determined that a redesign of the user interface was necessary to enhance overall user experience and streamline interaction flows.

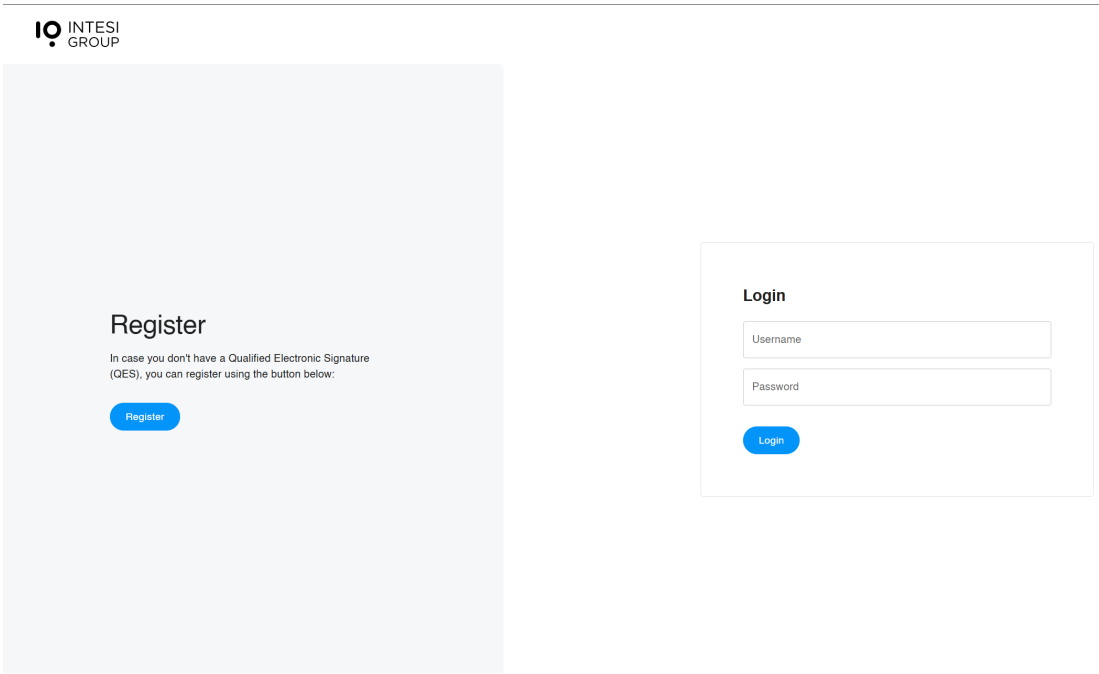
This redesign was executed in April 2025, resulting in a significantly improved user interface. The updated platform offers a more intuitive, responsive, and user-friendly experience, enabling users to navigate the signing process with greater ease and clarity.

Demonstration of the implementation

Recording of the implementation demonstrating the signing with the wallet

Format: Videos

Screenshots:



Co-funded by the European Union

INTESI GROUP

Verify Your Identity

To continue, verify your Person Identification Data (PID) using your EU Digital Identity Wallet. Scan the QR code or use the button below to open the app and confirm your identity.

EU Digital Identity Wallet

Scan the QR Code with your EUDI Wallet

Scan the QR Code with your EUDI Wallet

OR

Launch EUDI Wallet

Confirm Signing Credential Issuance:

2 Verify Identity

We need to Verify your Identity:

Scan the QR Code with your EUDI Wallet

OR

Launch EUDI Wallet

3 Signing Credential Issuance

Co-funded by the European Union

INTESI GROUP

Document Signing Service

Using the EU Digital Identity Wallet

Welcome to the Document Signing Service. Here you can securely sign your documents using your EU Digital Identity Wallet. This service ensures your identity is verified and your documents are signed with the highest level of trust and security. To get started, select or issue a signing credential, then upload your PDF document for signing.

EU Digital Identity Wallet

Your EUDI Wallet Certificate

Use your signing certificate to sign the document:

Signing Certificate 1

Select Other Certificate | Issue new Signing Certificate

Sign a PDF Document

Select a PDF file to sign.

Drag and drop a PDF file here, or click to select one

INTESI GROUP

Confirm Signing of Document

Verify your Identity using the EUDI Wallet

Documents to sign:

/ewc-signing-service-b… pdf 300kb

EU Digital Identity Wallet

Signing Confirmation

Please confirm the signing of the document you uploaded:

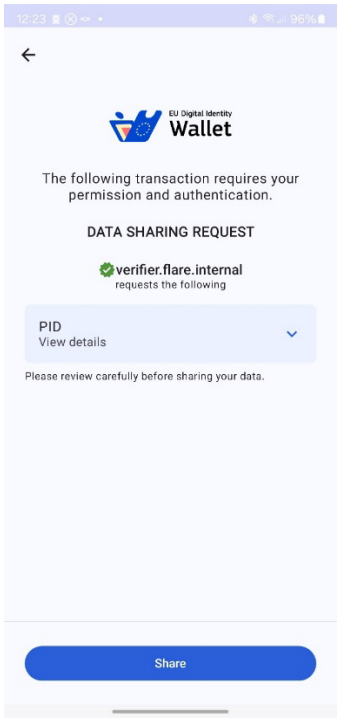
We need to Verify your Identity:

Scan the QR Code with your EUDI Wallet

OR

Launch EUDI Wallet

Co-funded by the European Union



Demo Site Link:

https://wallet.int4mind.com/signingservice

Conclusion, recommendations and next steps

The integration of the EU Digital Identity Wallet into Intesi Group Document Signing Service has proven effective within the EWC consortium. Through both user-initiated and Relying Party-initiated signing flows, the Wallet enables secure authentication and authorisation via SD-JWT-based PID presentation. The binding of a unique PID hash to each user account ensures that only the legitimate holder can perform key actions, such as certificate issuance and document signing.

Co-funded by the European Union

The system's reliability was confirmed through functional testing, which resulted in 37 successfully signed documents. In parallel, User Acceptance Testing involving developers and end-users led to a major interface redesign in April 2025, significantly enhancing usability and clarity of the signing process.

Moving forward, it is recommended to extend adoption to additional use cases, continuously align with evolving technical and regulatory standards, and maintain a strong focus on security monitoring and user feedback. These efforts will help ensure long-term sustainability and scalability of the solution.

A key recommendation is to move toward using the EU Digital Identity Wallet as the *sole* means of user authentication, replacing traditional credentials such as email and password, to simplify the user experience while maintaining a high level of trust and assurance.

This pilot demonstrates the practical value of the EU Digital Identity Wallet in delivering secure, efficient, and user-friendly digital services across borders.

Co-funded by the European Union

6.4 Annex – Signicat QES Integration

Operational Signing Services for EUDI Wallet

Name of the Provider: Signicat

Qualified Electronic Signatures

The integration uses one-shot, short-lived certificate issued from PID authentication. Signicat partners with the Norwegian qualified trust service provider Buypass for the pilot, using their Buypass BCSS[11] remote QES service providing the needed CSC API for the certificates and the hash signing. Signicat Sign[12] service runs the signing process, displaying documents to sign and capturing consent to sign. The user selects to sign with the EU Digital Identity Wallet and is redirected to an IDP, identity provider, Signicat's eID Broker[13], who performs the PID authentication and mediates the authenticated identity to Buypass BCSS for issuing of key pair and certificate.

Wallets used for testing

The signing is tested using the Thales NOBID Wallet implementation.

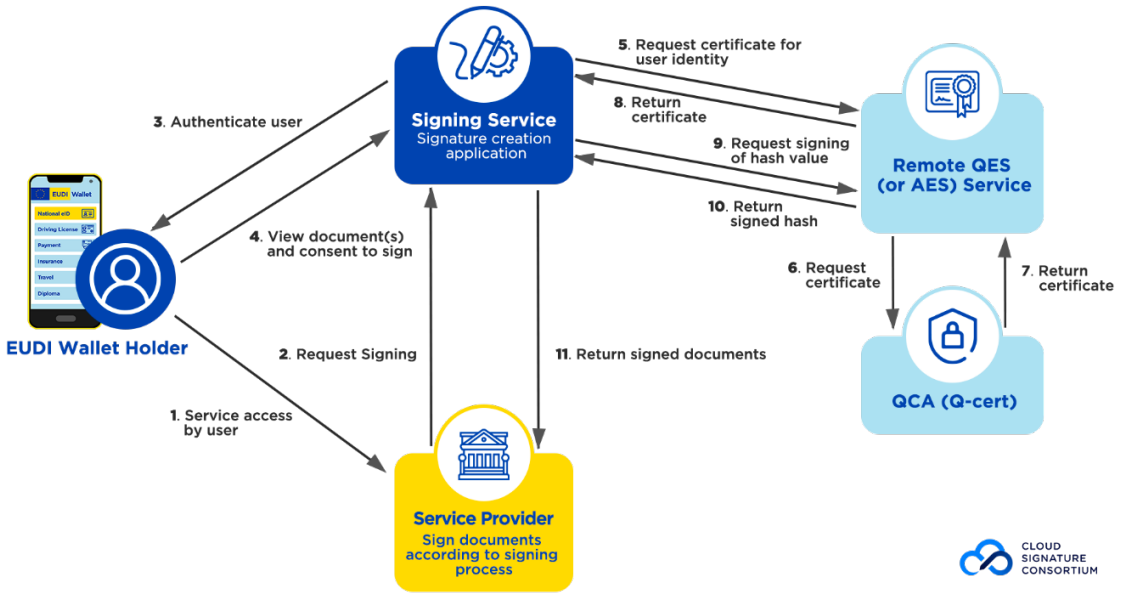
PIDs tested

The testing uses the PID attributes given name, family name, and date of birth.

Flows/Diagrams

The signing flow is a process of remotely signing a document using one-shot, short-lived certificates, handled by a Remote QES Service, as shown by the architecture in EWC Deliverable D4.8 clause 3.3.2 and Figure 2, copied below. Note however that the signing flow is a refinement of the flow in Deliverable D4.8 with several changes. The steps in the figure below are to some extent different from the flow tested. Notably, the figure does not show the IDP as a separate role but merged with the Signing Service (SCS).

[11] https://buypassdev.atlassian.net/wiki/spaces/BCSS/overview
[12] https://developer.signicat.com/docs/electronic-signing/sign-api-v2/
[13] https://developer.signicat.com/docs/eid-hub/



The flow has 5 main steps (note, different numbering from those in the figure above):

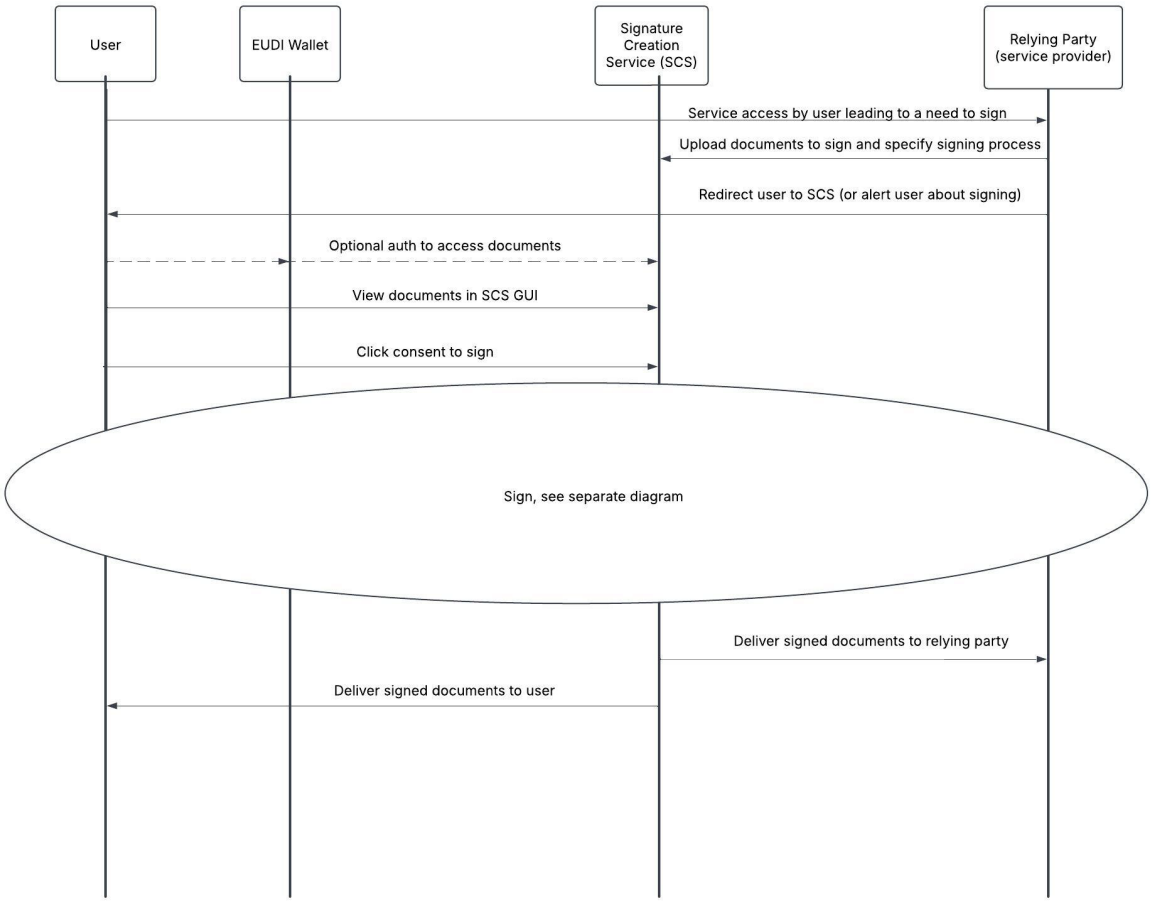
- Step 0: Service access by user leading to a need to sign - not detailed here.
- Step 1: Initiation of signature process by the service provider (relying party) in the signing service (SCS – Signature Creation Service) and access to the SCS by the user going through the signing process ending with consent to sign.
- Step 2: Create key pair and certificate, initiated by the SCS, resulting in a PID authentication transaction using the IDP and issuing of a certificate with subject identity derived from the authentication. The certificate is fetched by the SCS.
- Step 3: Compute DTBS/R (the hash value(s) to be signed), create SAD (Signature Activation Data), call the SSP to sign the DTBS/R (SCAL2 authorisation with the SAD), return signed hashes to the SCS.
- Step 4: Signature packaging into the desired ETSI xAdES format.
- Step 5: Delivery of signed documents to involved parties when all signers are done.

The flow description below is a generic description with the Remote QES Service using an “external” IDP (identity provider). The Buypass BCSS service has a slightly different setup as described at the end of this section.

Pre- and post-processing for signing

The figure below shows Step 1 and Step 5 of the flow above, with the other steps replaced by the oval and outlined afterwards.

Co-funded by the European Union



The Relying Party (RP) - usually a service provider of some kind but could be another user - requests signing of one or a set of documents. Documents are uploaded to the trusted Signature Creation Service (SCS), here Signicat Sign. The upload can be manual or using an API offered by the SCS, here an API is used. The API is proprietary. The CSC API is not relevant for this step.

The signing process is specified by configuration or API parameters to the SCS. The signing process specification governs aspects like which documents to sign (some may be only informational but must be read) and in what sequence, and not least how multiple signers are handled like any ordering of signers. The identity of the signer(s) will usually be mediated from the RP.

The SCS can be provided by the RP itself or by a trust service provider. An SCS falls under the eIDAS definition of a trust service (eIDAS Article 3 (16) (c)), but it cannot be a qualified trust service since there are no explicit eIDAS requirements for the service type. The SCS should conform to the ETSI TS 119 431-2 policy and security requirements standard. The SCS can provide its service “white labelled” giving the user the impression of signing at the RP, or it can be a branded service.

If the signing request originates from an online session with the user in the RP’s service, the user can be redirected to the SCS to sign in the same session (synchronous signing). In other cases, the user can be alerted that “there is a signing task waiting for you at the SCS” (asynchronous signing). In the case of multiple signers, only one of them can sign synchronously. However, future signers can be instructed to start from the RP’s site in the “waiting for” message, with subsequent redirection to the SCS.

Co-funded by the European Union

The user accesses the SCS. Depending on sensitivity of document content, authentication may be required to get access to documents. Authentication may or may not use the IDP that is used for signing; this authentication process is not detailed. The authentication may be by the user's EUDIW.

The user views documents in the GUI offered by the SCS according to the signing process specification. The user agrees to sign and confirms by clicking a "consent/sign" button in the SCS GUI. Consent can be one click for all documents or separate for each document depending on the signing process specification.

The consent triggers the signing flow described below.

After signing, the signed documents are delivered to the RP and/or the user. If there are multiple signers, the final delivery must be when all signers are done.

Signing process overview

The sequence diagram below shows the actions of the signing process starting after the user's click on "consent to sign" (Action 1 in the figure below). The main steps of the process are then done by the following actions:

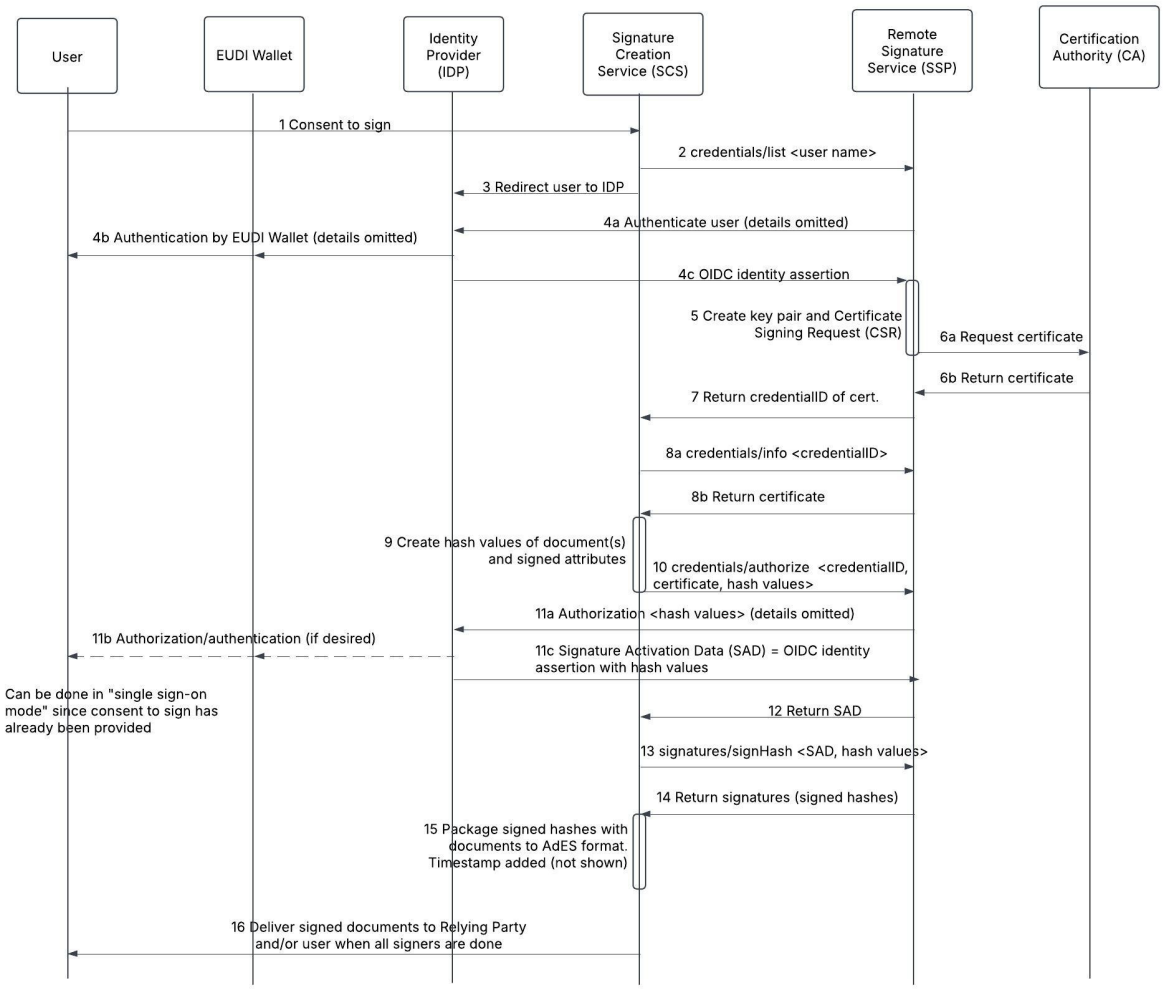
Step 2 create key pair and certificate: Actions 2-8b.

Step 3 create hash values to sign and sign them: Actions 9-14.

Step 4 packaging: Action 15.

The steps and actions are described below.

Co-funded by the European Union



Request key pair and certificate generation

The user's identity must be known to the SCS as user identification is a parameter for the call to the SSP to initiate certificate issuing: ***credentials/list <user name>*** (Action 2) according to the CSC API specification. This call returns all credentials (certificates) for the given user. Here, the call is interpreted as an instruction to create a key pair and issue a new certificate (credential) for the named user.

The ***user name*** parameter shall be reflected in the redirection from the SCS to the IDP to ensure that the authentication is linked to the correct credentials/list request. Further parameters to the ***credentials/list*** call may be used to secure the link between this call and the subsequent authentication.

Authenticate the user

In this flow, the Remote QES Service (SSP) is the actor that initiates the identity proofing of the user to whom the certificate shall be issued. The authentication protocol shall be an OAuth/OIDC flow. Format of assertions and OIDC flow are not detailed here. Actions are:

- Action 3: SCS redirects user to the IDP. The redirection shall be securely linked to the authentication request from the SSP. This can be by comparing user name or by other means.

Co-funded by the European Union

- Action 4a, 4b, 4c: The SSP requests authentication of the user (Action 4a). The IDP carries out PID authentication using the EUDIW (Action 4b). Attributes requested shall match the required certificate content. The final result is an OIDC identity assertion issued by the IDP (Action 4c).
- Action 5: The SSP creates a key pair and a certificate request (CSR) from the authenticated identity.
- Action 6a, 6b: The CSR is sent to the associated CA, who issues the certificate according to the selected certificate policy and certificate profile and returns the certificate, either user certificate only or complete chain, to the SSP.
- Action 7: The SSP answers the ***credentials/list <user name>*** call by returning the ***credentialID*** of the newly issued certificate to the SCS.
- Action 8a, 8b: The SCS retrieves the certificate using a ***credentials/info <credentialID>*** call to the SSP, who responds by returning the certificate, either user certificate only or complete chain.

Compute hash values to sign

The SCS now has all information for the hash value computation over document to sign and signed attributes, where the user certificate (optionally certificate chain) is a signed attribute according to the ETSI AdES standards (Action 9). This is why the certificate must be issued before the hash computation is done.

Request authorisation to sign resulting in SAD (Signature Activation Data)

In this flow, the SAD is a standard OIDC identity assertion for the user's name including also the hash values in the assertion. This is interpreted as the user's authorisation to sign these hash values. The OIDC assertion is issued by the trusted IDP.

The SCS calls the SSP for authorisation of signing by the CSC API call ***credentials/authorise <credentialID, certificate, hash values>*** (Action 10).

The SSP initiates an OAuth/OIDC call to the IDP (Action 11a). The call can use the same access token as the initial authentication to issue the certificate. The call must include the hash values and possibly other elements required for the SAD as "opaque" attributes that are just copied from the request to the identity assertion.

Details of the authentication/authorisation protocol are not specified here. Two alternatives exist at the IDP:

- Since the user has already explicitly consented to signing the documents (in Action 1), the identity assertion can be issued "silently" without user interaction resembling a single sign-on setup.
- If a new user interaction is deemed necessary, the user can be shown the hash values and the context for the authorisation and be asked to confirm by a new authentication using the EUDIW (Action 11b).

Displaying hash values is not user friendly and the consent to signing in Action 1 should be sufficient since the SCS is trusted to correctly compute hash values for the displayed documents.

Co-funded by the European Union

At the end, the SSP fetches an OIDC identity assertion for the user's identity containing also the opaque attributes from the authentication/authorisation request, at least the hash values to sign (Action 11c).

The SAD (the OIDC assertion) is returned to the SCS (Action 12) as response to the ***credentials/authorise <credentialID, certificate, hash values>*** call.

Sign the hash values

Next, the SCS issues a CSC API ***signature/signHash <SAD, hash values>*** call to the SSP (Action 13) to request signing of the hash values. The hash values must be the same as the hash values in the SAD (the OIDC assertion). Hash values and SAD are passed to the SAM (Signature Activation Module) within the CC certified (for QES) equipment operated by the SSP. The public key of the IDP must be configured in the SAM to validate the SAD and assure that it originates from a trusted IDP. Hence, SCAL2 (Sole Control Assurance Level 2) according to EN 419 241-1 is achieved to allow qualified signatures to be created.

The SSP signs the hash values using the private key associated with the certificate and returns the signed hashes to the SCS (Action 14) as response to the ***signature/signHash <SAD, hash values>*** call.

Signature packaging to AdES format

The SCS continues by packaging signed hash value with the document to sign and any unsigned attributes for all documents to sign. Packaging is to the requested ETSI AdES format (Action 15), typically PAdES for PDF documents. Since the certificate has a short lifetime, it is important that the signature is on a long-term format, B-T, B-LT, or B-LTA according to the ETSI AdES standards, applying a trusted timestamp before the certificate expires. For qualified signatures, a qualified timestamp should be used. The call to the (qualified) timestamp authority is not shown in the figures above.

If further signers are needed in the signing process, the process continues until all signers are done.

When all signers are done, the signed documents are delivered to the RP (the service provider) and/or the user (Action 16).

Alignment with EWC RFC010, variants and extensions

A main reason for using plain OAuth/OIDC for the PID authentication and authorisation actions in the present document is that this aligns with existing products in the market and allows the EUDI Wallet to be handled in the same way as other eIDs.

The signing flow in the present document can be modified to include issuing a QESAC (Qualified Electronic Signature Access Credential) as specified by EWC RFC010 as part of the PID authentication flow (Step 2 in the process). The QESAC could be used in the authorisation in Step 3 in the process.

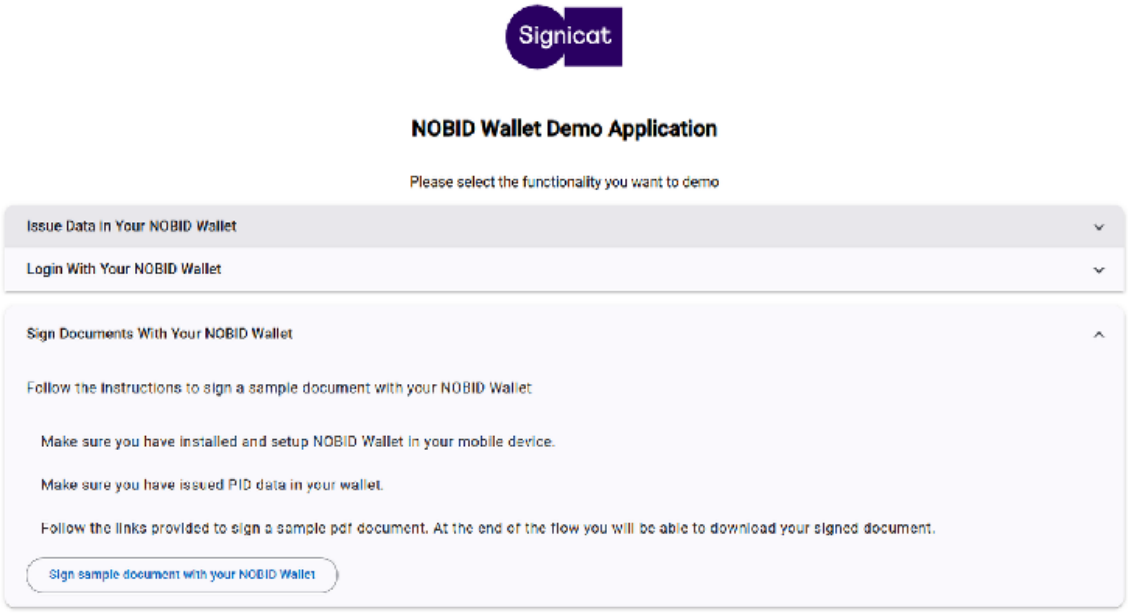
The use of the IDP can be replaced by direct interaction between the SSP and the user's EUDI Wallet as depicted by RFC010. Instead of going via the IDP for the authentication in Step 2 and the authorisation in Step 3, the SSP will directly interact with the user's EUDI Wallet for PID authentication to issue the certificate and to authorise creation of the SAD. This will however limit the flow to require all signers to have an EUDI Wallet. With an IDP, the same flow can be used by both EUDI Wallet users and users of other eIDs.

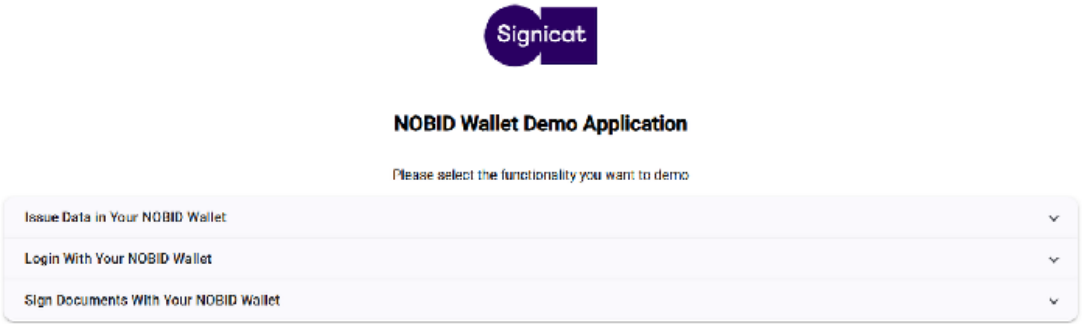
Co-funded by the European Union

Use of attribute attestations in the process in addition to PID authentication is an option that can be explored. An example is an attestation proving that the user is authorised to sign on behalf of a company, which could be used to add organizational attributes to the one-shot certificate.

Screenshots and user experience

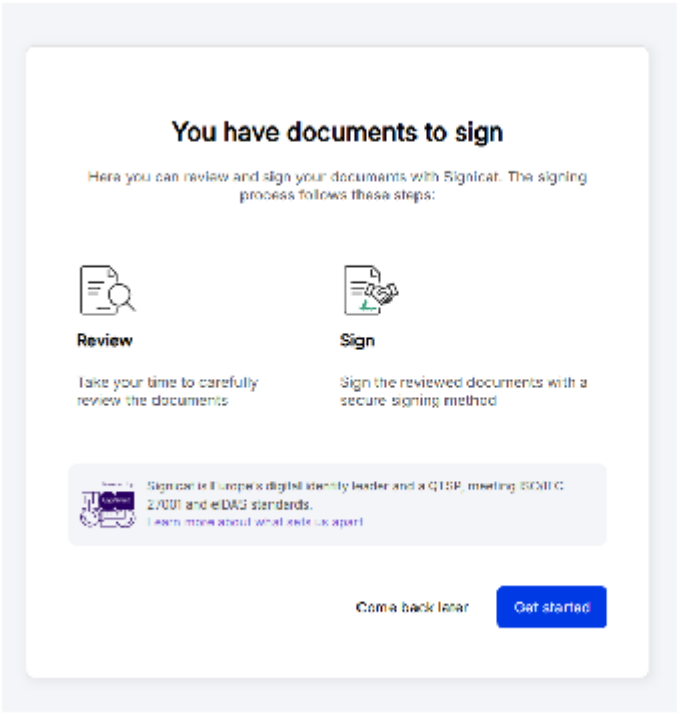
Testing at Signicat uses a simple demo application shared with the NOBID LSP at https://api.signicat.dev/wallet-poc/demo/start/ This is openly available and provides onboarding (issue data), authentication (with attributes), and signing. Clicking “Sign Documents” gives some instructions, notably that the user must have an EUDIW with identity data.

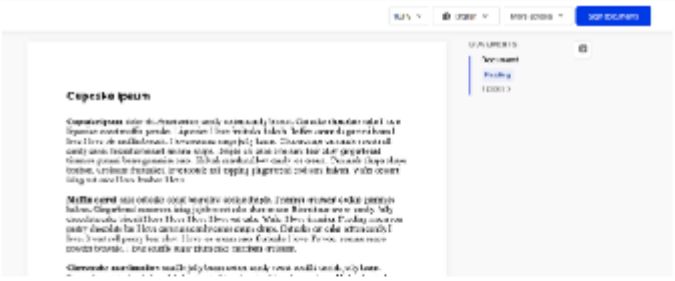


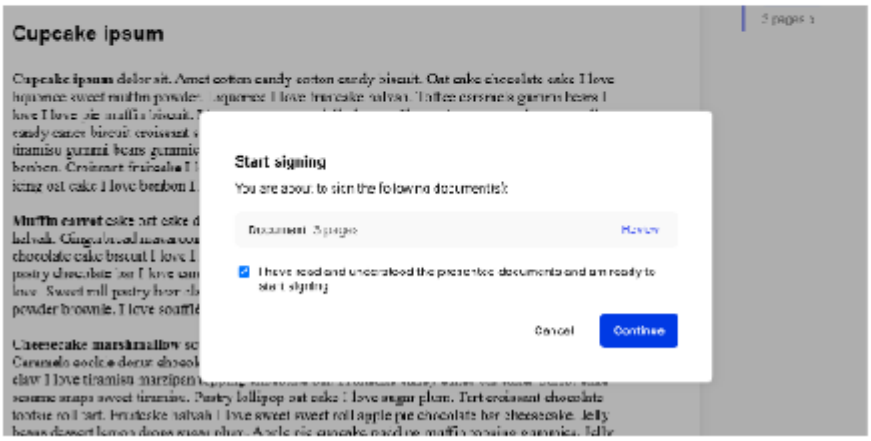


Clicking “Sign sample document” creates a sign session through the Signicat Sign API using a sample document and selecting via the API use of EUDIW to sign. There is currently no option to upload other documents. The user is redirected to Signicat Sign for the standard GUI start page of that service, and clicking “Get started” there gets you to the sign session. There, the document is read (but not the sample document with gibberish content), and one clicks on “Sign documents”, which sends the user to the confirmation screen. The “I have read and understood the document” button is ticked before clicking “Continue”. These steps are shown in the screenshots below.

Co-funded by the European Union

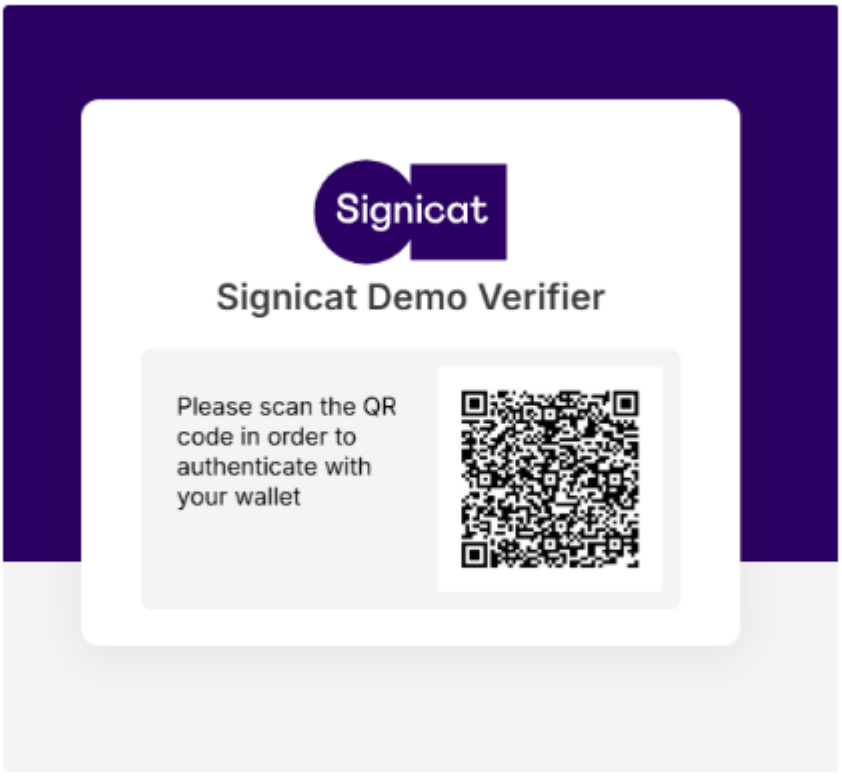




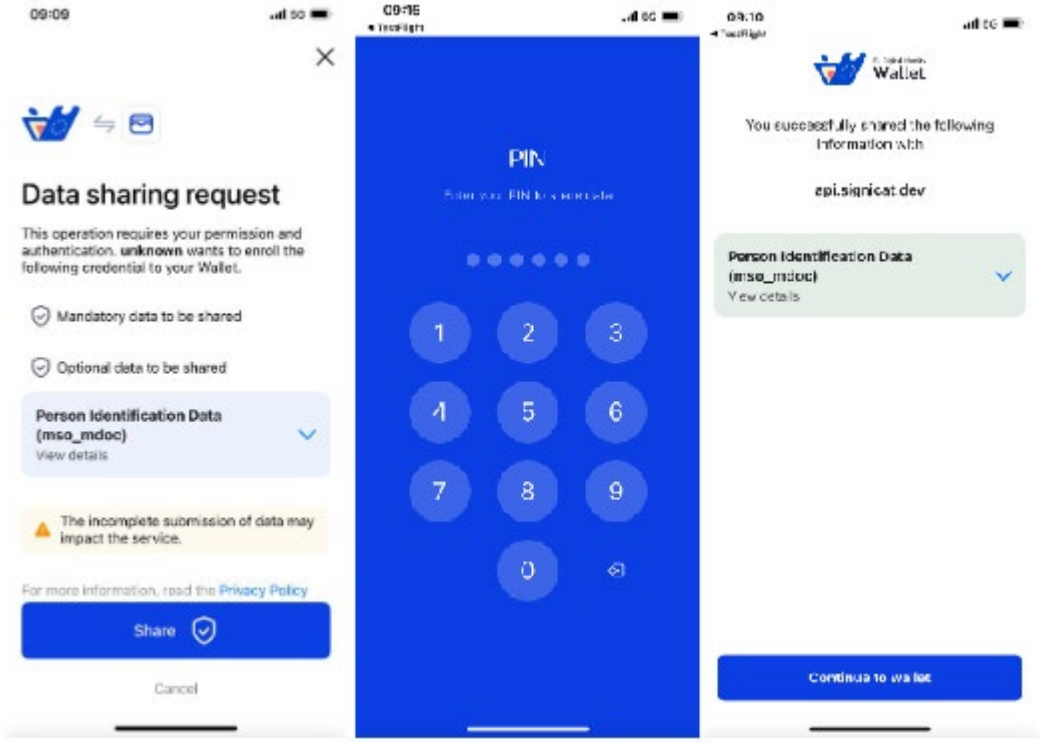


The user gets to the authentication dialogue in Signicat's Broker (the IDP) and is asked to authenticate with the EUDIW by scanning the QR code. The user runs a normal authentication, i.e. data sharing, dialogue in the app after scanning the QR code. Currently, the verifier asks for full name and date of birth.

Co-funded by the European Union

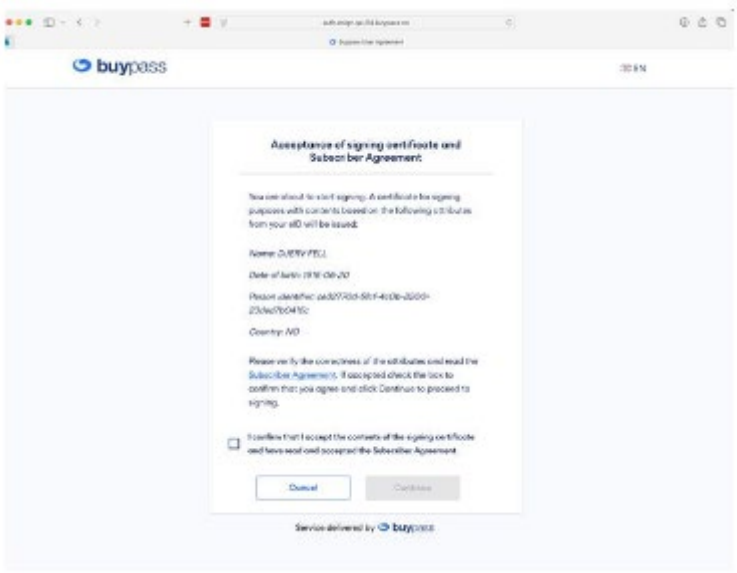


Screenshots of the the app dialogue below.



Co-funded by the European Union

Then, the user, in the web interface, must explicitly consent to Buypass as (qualified) trust service provider issuing a (one-shot) certificate for the identity. This is a requirement from applicable ETSI standards, where the term “subscriber agreement” comes from. The person identifier in the certificate is assigned by Buypass according to a Buypass numbering scheme. Alternatively, in later versions, the identifier could be an attribute from the Wallet, e.g. a national identity number or a national identity card number, see ETSI EN 319 412-1 for specification of the “semantic identifier” and use of the serial number attribute in subject names in certificates.



Following the consent, the key pair and certificate are issued, and the document is signed with no further user interaction. The last action (not shown) is that the user is redirected to a return-URI specified when the sign session was set up in the API, and the signed document can be retrieved and verified

Conclusion, recommendations and next steps

This setup may be the easiest possible for signing with the EUDIW. The advantage of using an SCS and an IDP is that signing flows can be set up where some signers use the EUDIW and other signers use other means. This will be important as other means will co-exist with the EUDIW for a long time.

Signature authorisation using authorisation by the EUDIW as described in RFC-010 is a fairly easy addition but must be supported by the Remote QES provider.

Multiple signers, multiple documents, and (part or total) sequencing of signers are inherent features of Signicat Sign and can be tested.

A beauty of one-shot certificates is that certificate content can be tailored to the context, e.g. using attributes relevant to the specific PID provided, possibly augmented by attribute attestations. Flexibility is however limited by what can be represented in an X.509 certificate.

The setup as described deprives the user of the option to select provider of Remote QES but simplifies the situation for the SCS (and the relying party) by only needing to integrate to one Remote QES provider. This can be extended to covering multiple QES providers and adding a selection menu.

Co-funded by the European Union

6.5 Annex – Validated ID QES Integration

Operational Signing Services for EUDI Wallet

Name of the Provider: Validated ID

Qualified Electronic Signatures

We have used a long-term certificate in our implementation, which the user has to setup beforehand and it's out of scope for this demonstration.

Wallets used for testing

We used our own wallet for testing, namely VIDwallet and ID Wallet LSP.

PIDs tested

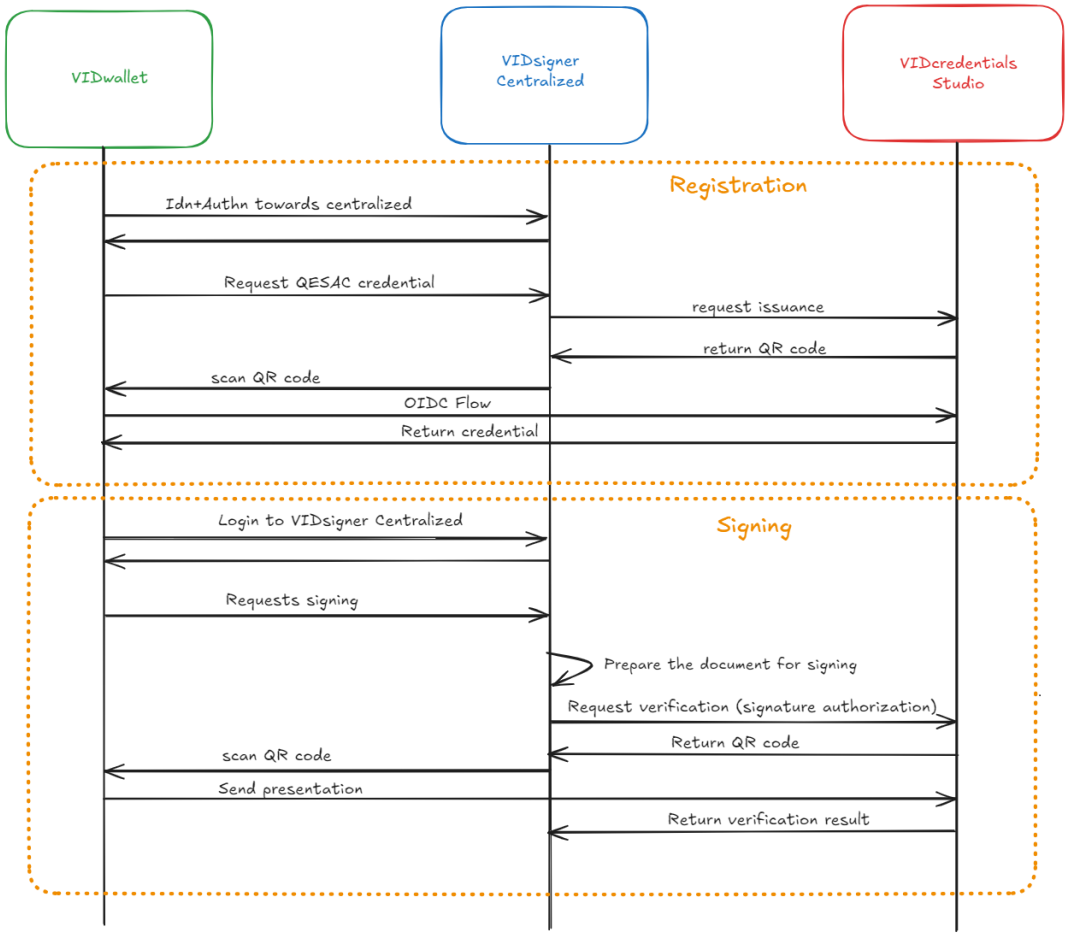
We did not use any PIDs within our user journey.

Flows/Diagrams

The use case that was implemented is the document signing with long-term certificates utilising an identity wallet. The use case consists of two main steps, namely the registration step and secondly the signing step.

1. In the registration step, the user logs into VIDsigner centralized and issues a QESAC credential that is used to bind the certificate ownership to a specific user with its identity wallet.
2. In the signing step, the user first reviews the document and then clicks on sign. A QR code is displayed which is scanned by the wallet and used to request the QESAC credential for authorising the signature.

Co-funded by the European Union



Co-funded by the European Union

Implementation

Validated IDs QES implementation using the identity wallet is based on the RFC eudi-wallet-rfcs/ewc-rfc010-long-term-certifice-qes-creation.md at main · EWC-consortium/eudi-wallet-rfcs that we have specified within EWC.

For the implementation, we have used our VIDsigner centralised platform that allows registered users utilizing long-term certificates to review and sign documents. Furthermore, we utilised our identity wallets namely VIDwallet and the ID Wallet LSP for the walk through of the user journey.

VIDsigner Centralized is Validated IDs remote signing service where registered users can use their long-term certificates to preview, review, and sign documents. More details there https://www.validatedid.com/en/centralized-signature. VIDsigner centralized integrates different remote qualified signing services (rQES). For this implementation, Validated IDs rQES was utilized.

VIDwallet is the identity wallet of Validated ID and was used during this implementation. VIDwallet follows the eIDAS2 and ARF developments and aims to be fully conformant. More details here https://www.validatedid.com/en/identity/vidwallet.

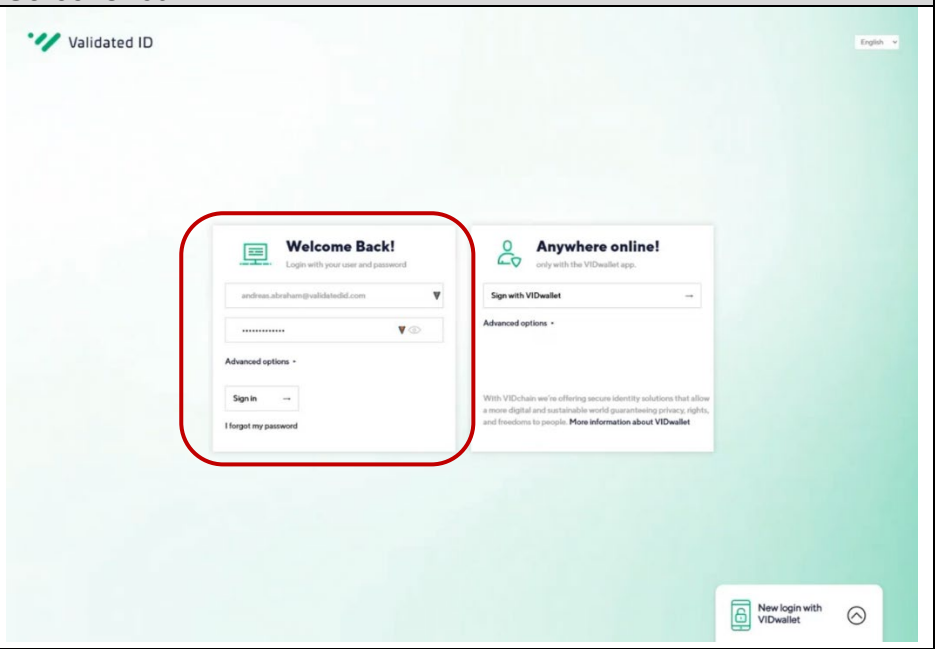
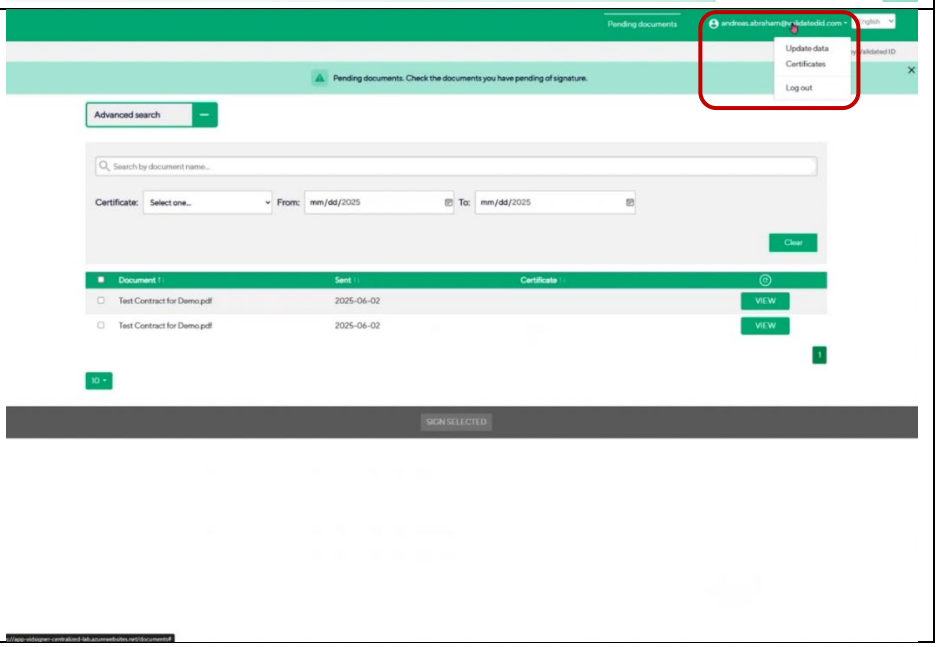
VIDcredentials Studio is the service that can be used by issuers and verifiers for performing the same processes. We used the studio to on the one hand issue the QESAC credential and on the other hand to request and verify the QESAC credential.

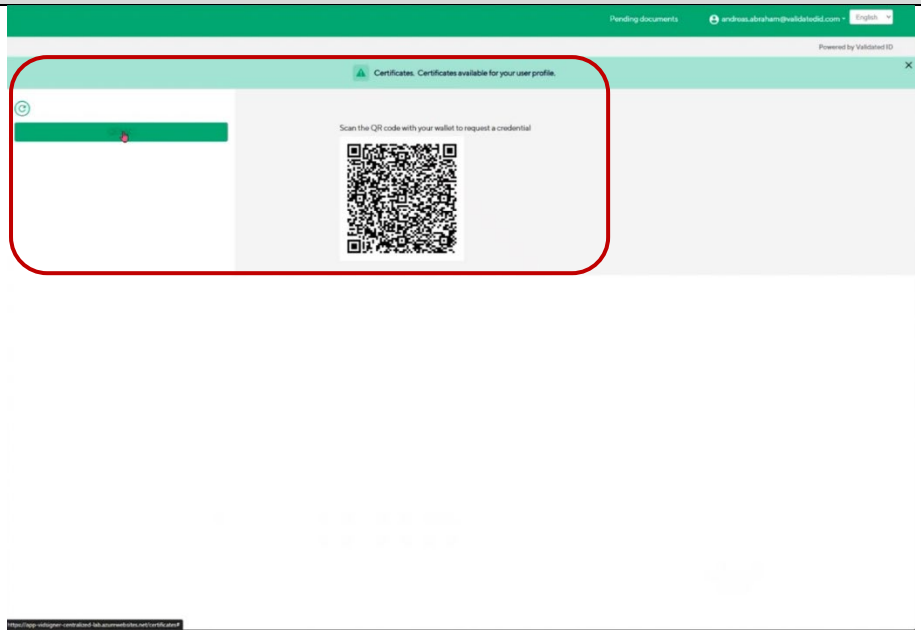
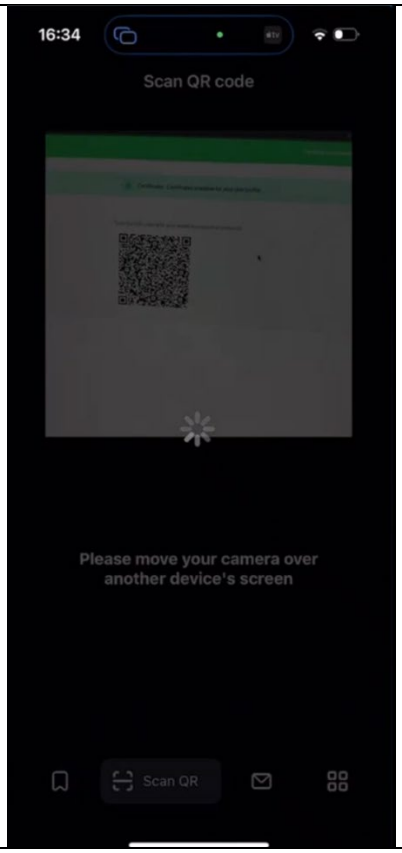
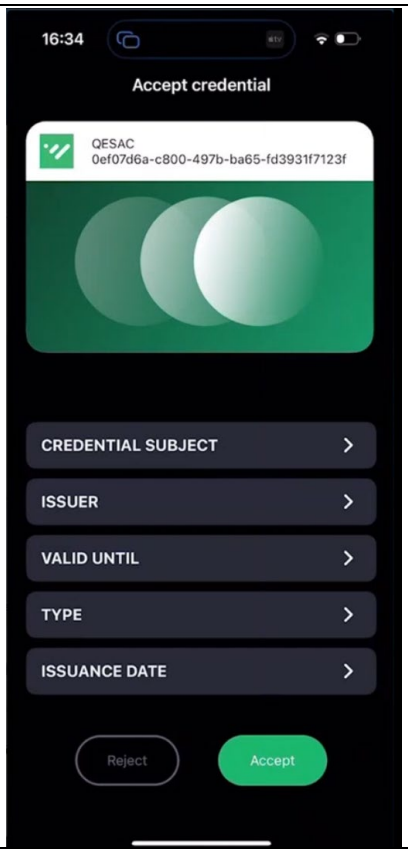
Co-funded by the European Union

Demonstration of the implementation

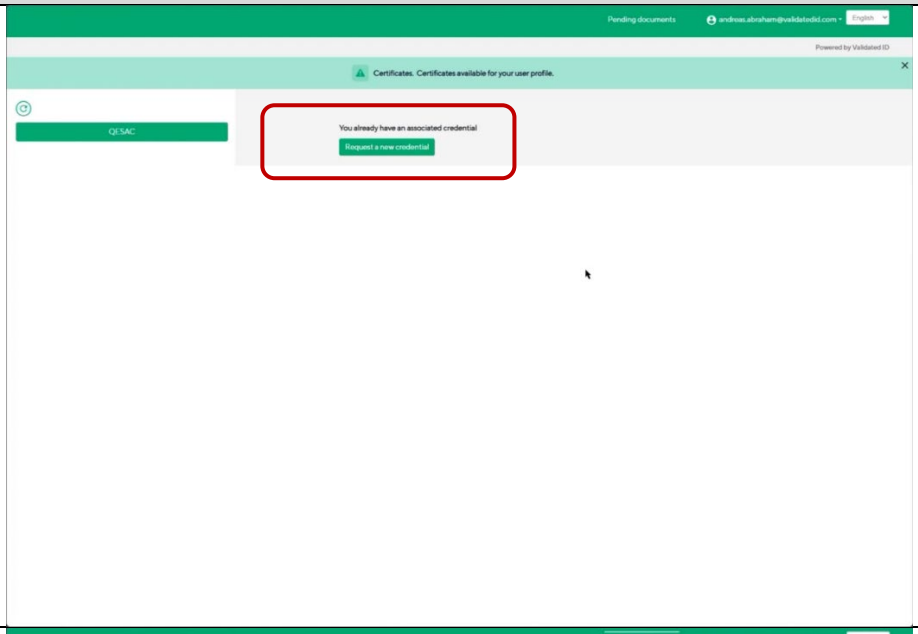
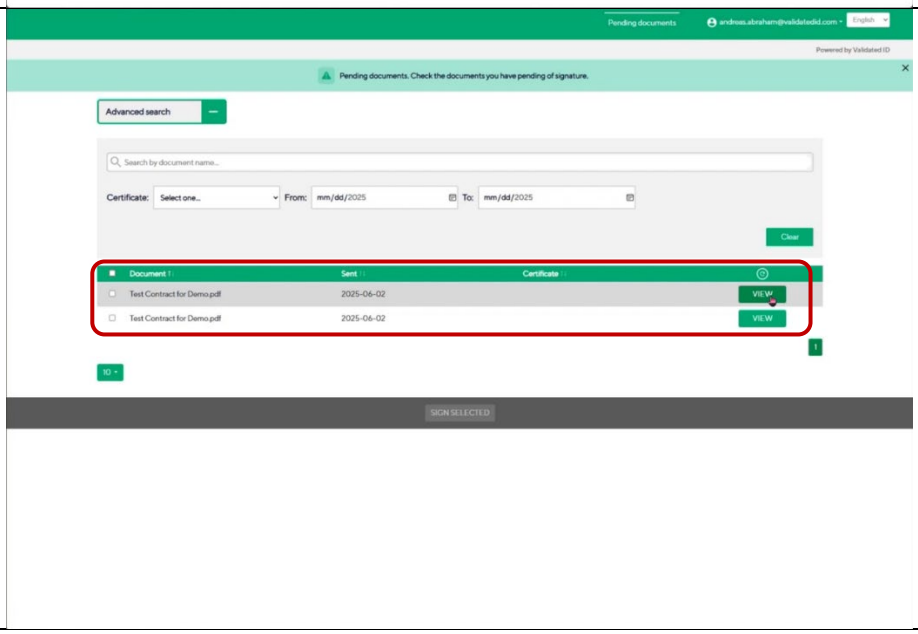
The recording of the full user journey is available here: https://nextcloud.ewc-consortium.eu/s/RNqQyimS5b2AjEj

Below, a series of screenshots provides a step-by-step walk through and explanation.

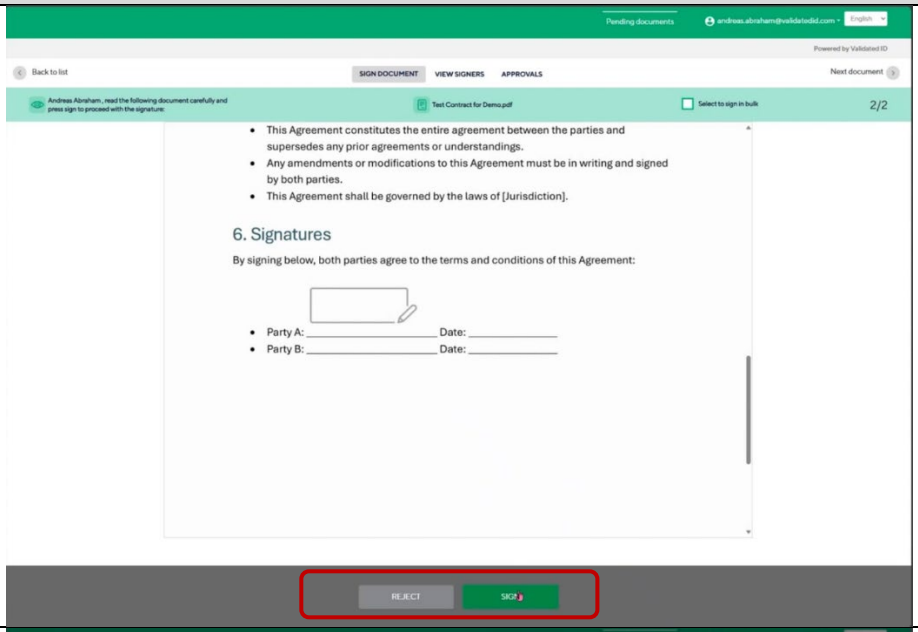
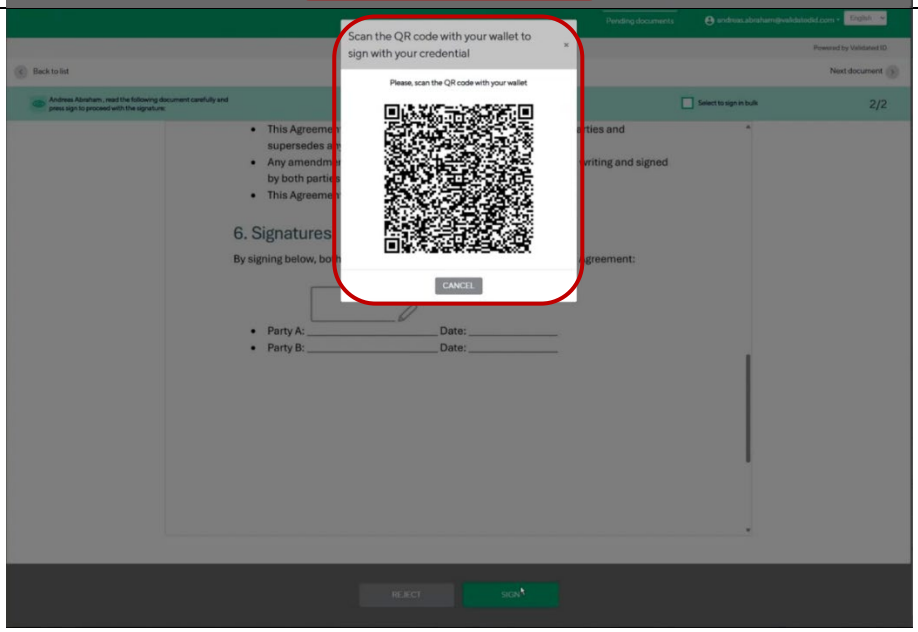
Description	Screenshot
On this first screenshot, the login page of VIDsigner Centralized singing services is displayed. We have two options for logging into the service, namely username and password as well as an identity wallet. For the user journey we chose the login with username and password assuming that the user is new to VIDsigner Centralized.	
After the user has logged in, they will click on the account settings and more specifically on the certificates section as shown on the screenshot.	

Description	Screenshot
On this screenshot we the certificates section of the logged in user. As shown on the picture, there is one certificate available and when clicking on that we could trigger the linking process between the selected certificate and the wallet. This is done through a QESAC credential that is issued into the users wallet as specified in the RFC010.	
Here, there are two screenshots shown of the wallet. The left one shows the wallet which is scanning the QR-code and processing the information. The second screenshot on the right side shows the QESAC credential that is sent to the wallet and the options for the user to either accept or reject this credential offer. After accepting it, the credential is stored in the wallet.	 

Co-funded by the European Union

Description	Screenshot
After successfully issuing the QESAC credential, we see the message besides the selected certificate that the certificate is already associated with a credential.	
On this screenshot, the main user interface of VIDsigner centralized is shown. Also, a list of documents to be singed are shown. Next, the user selects one document and clicks on view.	

Co-funded by the European Union

Description	Screenshot
The user now can review the document that is going to be singed. At the end of the page is the sign and reject button.	
On this final screenshot, the QR code is displayed which starts an OpenID connect for verifiable presentation flow in which VIDsigner centralized is requesting a QESAC credential in order to authorise the signature. The QR code is scanned in the wallet and the user confirms sharing the data. Finally, the signed PDF is ready.	

Conclusion, recommendations and next steps

Concluding Validated IDs implementation, it's worth mentioning that the implementation was a full success and a first step towards integrating the identity wallet in the signing processes.

As a next step, we will improve the current implementation focusing on user experience as well as allow the login to VIDsigner centralised with the PID. After that, we consider the implementation of the remote signing using the short-term certificate.

Co-funded by the European Union