Dissemination level: Public

EWC D3.6

BUSINESS SCENARIOS PILOT RESULTS AND EVALUATION

WP3

Author: UPRC, INVINET

Contributors: DFO, SCRO, OpenPeppol, TELESTO, VERO, ARCHIPELS, BRC, Infogreffe

Day of submission: 30/07/2025

Contents

Revisions 5

Executive Summary 6

List of abbreviations 7

1. Introduction 11

1.1 Scope and objective of deliverable 11

1.2 Methodology of work 11

1.3 Structure of the document 12

2. Methodology and Approach 12

2.1 Business scenario pilots 12

2.1.1 Identification of pilots 12

2.1.2 Pilot documentation structure 13

2.1.3 Pilot evaluation structure 13

2.2 Monitoring procedures 14

3. EWC Pilots Documentation 15

3.1 P1.1.1 Issue and verify attestations for evidence in the procurement process (ESPD) 15

3.1.1 Pilot description 15

3.1.2 State-of-the-art (SOTA) analysis 15

3.1.3 Business process overview and value 17

3.1.4 Architecture and infrastructure 18

3.2 P1.1.2 Automated verification of Economic Operator identity in the procurement process flow (ESPD) 19

3.2.1 Pilot description 19

3.2.2 State-of-the-art (SOTA) analysis 20

3.2.3 Business process overview and value 21

3.2.4 Architecture and infrastructure 23

3.3 P2.1.1 Onboarding new Business Partner 26

3.3.1 Pilot description 26

3.3.2 State-of-the-art (SOTA) analysis 28

3.3.3 Business process overview and value 28

3.3.4 Architecture and infrastructure 29

3.4 P2.2.1 Open a bank account for a business 31

3.4.1 Pilot description 31

3.4.2 State-of-the-art (SOTA) analysis 32

3.4.3 Business process overview and value 32

3.4.4 Architecture and infrastructure 34

Co-funded by the European Union

3.5 P4.1.1 KYS 2.0 Peppol network registration and use (Transforming Supplier Verification in eInvoicing) ... 37
3.5.1 Pilot description ... 37
3.5.2 State-of-the-art (SOTA) analysis ... 39
3.5.3 Business process overview and value ... 40
3.5.4 Architecture and infrastructure ... 41
3.6 P4.2.1 Verifiable eReceipt ... 43
3.6.1 Pilot description ... 43
3.6.1 State-of-the-art (SOTA) analysis ... 44
3.6.2 Business process overview and value ... 45
3.6.3 Architecture and infrastructure ... 47
3.7 P4.3.1 Create a company branch in another country ... 48
3.7.1 Pilot description ... 48
3.7.2 State-of-the-art (SOTA) analysis ... 50
3.7.3 Business process overview and value ... 52
3.7.4 Architecture and Infrastructure ... 54
3.8 P4.4.1 Company Authorized Business Travel and eInvoicing ... 55
3.8.1 Pilot description ... 55
3.8.2 State-of-the-art (SOTA) analysis ... 56
3.8.3 Business process overview and value ... 57
3.8.4 Architecture and infrastructure ... 58
4. EWC Pilots Evaluation ... 61
4.1 P1.1.1 Issue and verify attestations for evidence in the procurement process (ESPD) ... 61
4.1.1 Assessment summary ... 61
4.1.2 Pilot execution in production environment ... 63
4.1.3 Pilot user testing feedback ... 63
4.1.4 Insight and lessons learnt ... 64
4.1.5 Recommendations ... 65
4.2 P1.1.2 Automated verification of Economic Operator identity in the procurement process flow (ESPD) ... 65
4.2.1 Assessment summary ... 65
4.2.2 Pilot execution in production environment ... 67
4.2.3 Pilot user testing feedback ... 67
4.2.4 Insights and lessons learnt ... 68
4.2.5 Recommendations ... 68
4.3 P2.1.1 Onboarding new business partner ... 69
4.3.1 Assessment summary ... 69

4.3.2 Insights and lessons learnt ... 69
4.3.3 Recommendations ... 70
4.4 P2.2.1 Open a bank account for a business ... 70
4.4.1 Assessment summary ... 70
4.4.2 Pilot execution in production environment ... 72
4.4.3 Pilot user testing feedback ... 73
4.4.4 Insights and lessons learnt ... 74
4.4.5 Recommendations ... 78
4.5 P4.1.1 KYS 2.0 Peppol network registration and use ... 79
4.5.1 Assessment summary ... 79
4.5.2 Pilot execution in production environment ... 80
4.5.3 Pilot user testing feedback ... 81
4.5.4 Insights and lessons learnt ... 81
4.5.5 Recommendations ... 83
4.6 P4.2.1 Verifiable eReceipt ... 83
4.6.1 Assessment summary ... 83
4.6.2 Pilot execution in production environment ... 86
4.6.3 Pilot user testing feedback ... 87
4.6.4 Insights and lessons learnt ... 87
4.6.5 Recommendations ... 88
4.7 P4.3.1 Create a company branch in another country ... 88
4.7.1 Assessment summary ... 88
4.7.2 Pilot execution in production environment ... 89
4.7.3 Pilot user testing feedback ... 89
4.7.4 Insights and lessons learnt ... 90
4.7.5 Recommendations ... 96
4.8 P4.4.1 Company authorized business travel and eInvoicing ... 98
4.8.1 Assessment summary ... 98
4.8.2 Pilot execution in production environment ... 99
4.8.3 Pilot user testing feedback ... 100
4.8.4 Insights and lessons learnt ... 100
4.8.5 Recommendations ... 101
5. Conclusions ... 101
5.1 Final pilot results ... 101
5.2 Summary of attestations and wallets used ... 102
5.3 Concluding remarks and recommendations ... 103
Annex A: User Journey Screenshots ... 106

Company Verification process – B2BRouter Verifier 106
Fast Ferries / Vero – vReceipt interfaces 113
Annex B: User Testing Feedback...118
Open a bank account – Digital Wallet Trial User Feedback form 118
Create a company branch – Testing..119

Revisions

Version	Date	Author	Changes
v0.1	09.06.25	UPRC	Initial draft version
v0.3	15.07.25	INVINET	Integrated contributions from all partners
v0.8	22.07.25	UPRC	Ready for review by the Management Board (MB)
v0.9	28.07.25	UPRC	Updated taking into account Management Board (MB) comments

Executive Summary

Deliverable D3.6, titled “**Business Scenarios Pilot Results and Evaluation**”, documents the final implementation and evaluation of business scenario piloting activities conducted within the EU Digital Identity Wallet Consortium (EWC), under Work Package 3 (WP3). It takes as a basis the pilot plans, defined goals, ambition levels and KPIs defined in deliverable D3.5 and presents outcomes from phases 3 to 5 of the pilot lifecycle: Technical Design and Implementation, Operations and Measurement, and Evaluation, Sustainability, and Handover.

The final version of D3.6 reflects the completed status of the pilots’ documentation and their outcomes.

Eight business scenario pilots (**seven** defined in D3.5 and a **new one** added in the deliverable) were implemented and assessed, reflecting real-world applications of the European Digital Identity Wallet (EUDIW) for Legal Persons.

Each pilot was evaluated against its stated goals, ambition levels, key performance indicators (KPIs), and user feedback. The results offer insights into the feasibility and impact of digital wallet use in various sectors, including procurement, banking, eInvoicing, business registration, and corporate travel.

Key achievements include:

- Demonstrated reduction of administrative burden and fraud risk in cross-border public procurement processes.
- Simplification of onboarding and identity verification for business partners and suppliers.
- Streamlined, secure KYC/KYS (Know Your Customer/Supplier) procedures in banking and eInvoicing contexts.
- Validation of the EUDIW as a tool for improving compliance, trust, and efficiency across multiple business functions.

The pilots highlighted both the potential and limitations of current technologies and regulatory readiness. Notably, the integration of verifiable credentials and trusted issuers via digital wallets showed significant promise in enhancing data authenticity, automation, and interoperability across Member States. Feedback from participating companies in the EWC pilots has clearly indicated the importance of enabling organisations to use wallets for their business transactions – whether with other companies, individuals, or public authorities – across the EU. The potential for the use of business wallets is huge and the business wallet can really be a game changer for wider adoption and uptake of the wallet ecosystem.

D3.6 concludes with **insights and lessons learned**, and **recommendations** for each of the implemented piloting solutions. These findings support the future adoption and policy development around the European Digital Identity Wallet and European Business Wallet (the latest being announced by the president of European Commission in the Competitiveness Compass in January 2025) and its role in fostering a seamless digital single market, but they also highlight what still needs to be done for the deployment and uptake of the business wallet ecosystem.

List of abbreviations

Acronym	Explanation
(Q)EAA	(Qualified) Electronic Attestation of Attribute
AI	Artificial Intelligence
AML	Anti Money Laundering
API	Application Programming Interface
ARF	Architecture and Reference Framework
AS	Aksjeselskap
ASA	Allmennaksjeselskap
B2B	Business to Business
BORIS	Beneficial Ownership Registers Interconnection System
BR	Brønnøysundregistrene
BRIS	Business Register Interconnection System
BRREG	Brønnøysund Register Centre
BTRL	Banca Transilvania
CA	Contracting Authority
CEN/TS	European Committee for Standardization / Technical Specification
CEPPR	Central Electronic Public Procurement Registry
CIR	Commission Implementing Regulation
CNGTC	Conseil National des Greffiers des Tribunaux de Commerce
CSRF	Cross-Site Request Forgery
DFØ	Direktoratet for Forvaltning og Økonomistyring
DUNS	Data Universal Numbering System
DVV	Digi- ja väestötietovirasto - Digital and Population Data Services Agency
e-SENS	European Simple Electronic Networked Services Large Scale Pilot project
EAA	Electronic Attestation of Attributes
EAS	Electronic Address Scheme
EBSI	European Blockchain Services Infrastructure
EC	European Commission

Co-funded by the European Union

Acronym	Explanation
EDM	Exchange Data Model
EEA	European Economic Area
eID	electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
EN	European Norm
ENISA	European Network and Information Security Agency
EO	Economic Operator
ESPD	European Single Procurement Document
ETSI	European Telecommunications Standards Institute
EU	European Union
EUBW	European Business Wallet
EUCC	European Company Certificate
EUDI	European Digital Identity
EUDIW	European Digital Identity Wallet
EWC	EU Digital Wallet Consortium
FOSS	Free and Open Source Software
FTE	Full time Equivalent
GA	General Assembly
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
IBAN	International Bank Account Number
ID	Identifier
IT	Information Technology
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KVK	Kamer van Koophandel
KYC	Know Your Customer
KYS	Know Your Supplier
LEI	Legal Entity Identifier
LoA	Level of Assurance

Acronym	Explanation
LPID	Legal Person Identification Data
LSP	Large Scale Pilot
M	Month
MDG	Ministry of Digital Governance
mDoc	Mobile Document
MS	Member State
N/A	Not Available
NEPPS	National eProcurement System
ODI	Organizational Digital Identity
OOTS	Once-Only Technical System
PEPPOL	Pan-European Public Procurement Online
PID	Person Identification Data
POS	Point of Sale
QEAA	Qualified Electronic Attestation of Attributes
QES	Qualified Electronic Signatures
QR	Quick-Response
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
QWAC	Qualified Web Authentication Certificates
SD-JWT	Selective Disclosure for JWTs (JSON Web Tokens)
SDGR	Single Digital Gateway Regulation
SDK	Software Development Kit
SE	Societas Europaea
SME	Small and Medium-sized Enterprise
SOTA	State Of The Art
SQL	Structured Query Language
TOOP	The Once-Only Principle Large Scale Pilot project
UBO	Ultimate Beneficial Owner
UI	User Interface
UPRC	University of Piraeus Research Centre

Acronym	Explanation
USD	United States Dollar
UX	User Experience
VAT	Value Added Tax
VC	Verifiable Credentials
WP	Work Package

1. Introduction

D3.6 Business scenarios pilot results and evaluation delivered by: WP3 / Task 3.3

Date: 31 July 2025

Type: Document, Report

Classification: Public

Lead beneficiary: UPRC

1.1 Scope and objective of deliverable

The purpose of deliverable D3.6 “Business scenarios pilot results and evaluation” is to provide a final overview of the WP3 business scenario pilot activities done within the EWC. Specifically, this deliverable presents:

1. Updates on the evolution and implementation of WP3 business scenario pilot plans up to the end of the project (July 2025)
2. An evaluation of each business scenario pilot, including performance against defined goals, ambition levels, and KPIs.

This document builds upon the information presented in D3.5 and incorporates input gathered through interim monitoring of the business scenario pilots. The final version reflects the completed status of the pilots, their outcomes and lessons learned.

D3.6 presents the **documentation** of the result from phase 3 “Technical design and implementation of pilots”, phase 4 “Operations and measurement” and phase 5 “Evaluation, sustainability, and handover” of the Pilot Lifecycle defined in D3.5, which constitute the content of piloting subtask T3.3.2 Business Scenario Pilot implementation, Running & Evaluation within the WP3 workplan under task T3.3 Business Scenarios Piloting.

Out of the nine business scenario pilot plans formulated in D3.5, the seven of them proceeded with implementation. Since the writing of D3.5, one additional pilot plan called “Company Authorized Business Travel and eInvoicing” was identified and implemented, bringing the total number of business scenario pilots implemented to eight. This new pilot was developed following the same evaluation approach as the others.

1.2 Methodology of work

The methodology used to produce the present deliverable and achieve its outlined objectives followed an iterative approach, designed to ensure timely updates and accurate reporting. The process started with pilot participants reporting progress of the business scenario pilots documented in D3.5, using a structured word template and guidelines shared by the WP3 lead during bi-weekly calls. In February 2025, all pilot participants were asked to submit their updates using a provided pilot documentation template. The collected pilot plan updates and documentation were compiled into an internal version of the deliverable, which served as a working document to track the ongoing evolution of the pilots. In June 2025, participants were asked to provide final updates on both implementation and evaluation of their pilots. This final round of input resulted in the final preparation of D3.6, which consolidates the full documentation and evaluation of all ten pilots.

A detailed description of the methodology is provided in chapter 2.

1.3 Structure of the document

The document is structured as follows:

Chapter 1 introduces the deliverable by outlining the scope and objectives of the deliverable and an overview of the methodology used in the context of the deliverable.

Chapter 2 presents the methodology of work, including definition of the pilot documentation and evaluation.

Chapter 3 presents the documentation of the business scenario pilots

Chapter 4 presents the evaluation of each business scenario pilot, including performance against defined goals, ambition levels, KPIs and lessons learnt concluding with some key recommendations.

Chapter 5 presents an overview of the wallets and attestations used in each business scenario pilot, and some final conclusions and reflections on the work done in piloting ODI/Legal Person Identity in EWC and recommendations for deployment and uptake of the business wallet ecosystem.

2. Methodology and Approach

The piloting methodology as well as the pilot lifecycle adopted in EWC for the ODI business scenarios piloting is described extensively in deliverable D3.5.

2.1 Business scenario pilots

2.1.1 Identification of pilots

The table below shows the complete mapping from Business Areas to Business Scenarios and Pilot Plans as defined in deliverable D3.5.

Table 1 EWC ODI business areas, business scenarios and pilot plans

Business Areas	Business Scenarios	Pilot Plans
BA1 - Public Procurement	**BS1.1** - Public procurement	**P1.1.1** - Issue and verify attestations for evidence in the procurement process (ESPD)
		P1.1.2 - Automated verification of Economic Operator identity and mandate in the ESPD
BA2 - Know Your Supplier	**BS2.1** - Know your business partner	**P2.1.1** - Onboarding new business partner
	BS2.2 - Know your customer (KYC)	**P2.2.1** - Open a bank account for a business
BA3 - Domain Registration	**BS3.1** - Domain holder verification by domain registry	**P 3.1.1** - Domain holder verification by domain registry
	BS3.2 - Domain ownership as credential for QWAC issuance	**P3.2.1** - Domain ownership as credential for QWAC issuance
BA4 - Business Document Exchange	**BS4.1** - Peppol network registration and use	**P4.1.1** - Peppol network registration and use
	BS4.2 - Verifiable eReceipt	**P4.2.1** - Verifiable eReceipt
	BS4.3 - Create a company branch in another country	**P4.3.1** - Create a company branch in another country

Since the writing of D3.5, a new pilot has been introduced in BA4 – Business Document Exchange under the code "**P4.4.1 Company authorized business travel and eInvoicing**".

As part of the ongoing monitoring and assessment of business scenario pilots, participants were regularly asked to provide updates on their implementations in the biweekly calls, and also to provide an interim documentation in February 2025, using a structured pilot documentation template. Finally, participants were asked to provide their final documentation updates, as well as a structured evaluation for their pilots which culminated to the final version of D3.6.

The structure of the template used to collect input and monitor the ongoing efforts is presented in the following section.

2.1.2 Pilot documentation structure

Each business scenario pilot documentation includes the following sections:

- **Pilot basic information:** this section captures basic information such as the pilot's name and the names of the EWC partners involved.
- **Pilot extended description:** where the pilot participants are asked to provide more in-depth details of the pilot such as the current pilot scope, motivation and goals, state-of-the-art analysis, business process overview, business value and an overview diagram of architecture topology and infrastructure.
- **KPIs:** This section includes reporting of the current KPIs including metrics such as the number of relying parties, wallet users, and number of transactions completed.

2.1.3 Pilot evaluation structure

The pilot evaluation framework used in EWC is based on the pilot evaluation framework that was used in TOOP, PEPPOL and e-SENS and it was suitably modified and adapted for EWC. Each pilot evaluation includes the following sections:

- **Assessment summary**: this section presents how each pilot was **evaluated against its own goals** set in the pilot plan included in the deliverable D3.5, and an **overall assessment and evaluation of ambition level achievement (KPIs).**
- **Pilot execution in production environment**: where the pilot participants are asked to describe how close to real-life systems the piloted systems are.
- **Pilot user testing feedback**: where the pilot participants are asked to provide details on the pilot user testing and feedback (if applicable)
- **Insights and lessons learnt:** where the pilot participants describe insights and high-level issues encountered during piloting activities, and what they have learned so far.
- **Recommendations:** this paragraph concludes with some recommendations for scaling the business wallet in the piloting domain.

The aim of pilot evaluation is to assess whether and to what extend the initial goals and objectives have been met by each business scenario pilot.

In the context of deliverable D3.5, all business scenario pilots were requested to declare their level of ambition in each pilot, and it was then aggregated at WP3 level.

In the context of the pilot evaluation, all WP3 pilots implemented are requested to declare their achieved level with regard to KPIs defined in deliverable D3.5. Thus, the ambition level planned is compared with the corresponding achieved level.

Co-funded by
the European Union

Pilot execution in production environment: Here qualitative data are collected with regard to how close to real-life systems the systems that participate in piloting are. The pilots are asked to specify with what systems are working: production or pre-production/acceptance environments or clones of the production systems, built on purpose for the pilots or new prototypes built for the pilot.

Therefore, the different categories considered are the following:

- **Production**: the system connected is the one in production.
- **Pre-production/acceptance**: the system connected is the one that is used by the organisation as pre-production and acceptance environment for any changes/updates on the production environment.
- **Clone of production built for the pilot**: the system connected is a clone of the production system built for the pilot. This is an option preferred by some organisations in order to have a separate development environment to try new functionalities depending on the policy (e.g., security constrains) of the organisation. From our perspective, we consider this type the same as the pre-production/acceptance environment.
- **New prototype built for the pilot**: the system connected is a new prototype that was built specifically for the pilot. This specific category includes the pilots that did not have a system in production before the pilots, and they built the prototype in order to connect and to later use this prototype in production once successfully showing the functionality. This category does not count in the systems that are either in production, or close to production environment.

Established pre-production or acceptance environments or clones of the production systems, built on purpose for the pilots are customary methods for building new services and testing them before they are put into real production.

2.2 Monitoring procedures

Pilots develop at different speeds due to the diverse contexts within they are operated. This variety emphasizes the importance of ongoing monitoring throughout a pilot lifecycle. To effectively monitor this dynamic landscape, distinct pilot states were defined in D3.5 to capture the progression of the pilot initiatives.

The defined in D3.5 states can be summarized in the Table 2 below. The colour-coordination serves to underline how a pilot gets closer to full readiness across its lifecycle. Detailed state descriptions are available at section 2.4 of D3.5.

Table 2 Pilot lifecycle state colour coordination

🟧	Not started/commitment to be confirmed
🟨	Commitment/ready to start implementation
🟩	In progress
🟩	Technical readiness achieved

This grading of pilot state was used during the course of the project for reporting the business scenario pilot status.

3. EWC Pilots Documentation

This chapter outlines the final updated documentation of the eight business scenario pilots that proceeded in implementation (seven pilots were originally committed to by the beneficiaries, based on the pilot plans defined in deliverable D3.5, and one additional pilot called “Company Authorized Business Travel and eInvoicing” that was identified later and implemented).

3.1 P1.1.1 Issue and verify attestations for evidence in the procurement process (ESPD)

3.1.1 Pilot description

Selection criteria are the minimum requirements or standards that bidders in public procurement must meet. These are economic and financial standings; professional and technical knowledge or ability and rejection factors such as bankruptcy. From a policy perspective there is a lot of focus on the need to use the same mechanism to ensure that requirements within environmental and social responsibility areas are also met, not just at the start of a project but throughout the whole contract period.

The “classic” way of document this is to provide certificates and statements issued by both private and public actors, such as an ISO27001 or tax certificate, usually in PDF format. In sum these certificates are the “proof of business”.

By using an EUDIW we aim to make it easy for a legal entity to collect, use and share continuously authentic and up to date certificates needed within their area of business, piloted/proved through the use within a public procurement project.

EWC partners involved:

- Direktoratet for forvaltning og økonomistyring (DFO) (The Norwegian Agency for Public and Financial Management)
- Brønnøysundregistrene (BR) (The Norwegian Register of Business Enterprises)
- iGrant
- Skatteetaten (Norwegian Tax Administration)

The **pilot idea** is to utilize EUDIW for organizations to easily document that they meet the selection criteria in a given public procurement project.

For this pilot we have made the assumption that access to and infrastructure necessary for a functioning wallet is in place, so that part of the process is out of scope.

The **motivation and goals of the pilot** are the following:

1. How public authorities can issue certificates that are verifiable, authentic, and always up to date.
2. How a legal entity can collect, use, and share certificates using the EUDIW.
3. How public contractors can use EUDIW to trust that their contracts are performed as agreed.

3.1.2 State-of-the-art (SOTA) analysis

The most common method in Norway today:

Certificates for organizations are collected from various public and private sources, usually as a PDF file. Tax certificates are downloaded from an official digital portal, Altinn, using digital ID log in. Altinn has predefined roles that organizations can dedicate to their employees. The various roles give the user right to access certain documentation.

Official digital evidence service called eBevis (translates as "eEvidence")

eBevis is a collaboration between Brønnøysundregistrene, the Tax Administration, the Directorate of Digitalisation, and DFØ. The solution was launched on 01.04.19.

eBevis is a solution designed to digitize the procurement process, and it is also used as a tool to verify whether suppliers are legitimate. eBevis allows public contracting authorities/purchasers to access and retrieve defined real-time data about suppliers in connection with public procurements.

Through the consent solution in Altinn, the system can collect and provide non-public data, such as tax information.

The service has several limitations. It is only accessible via the tender platforms Artifik and Mercell. It can only be used by public contractors during a tender process before a contract is signed, and not during the contracting period. eBevis collects evidence from Brønnøysundregistrene, the Tax administration, Norwegian Public Roads Administration and Norwegian Labour Inspection Authority, collecting data on approved cleaning and car detailing businesses in addition to business certificates and tax information. Of the two tender platforms only Artifik has implemented the data from all sources, but this didn't happen until late 2024. Mercell has only implemented data from Brønnøysund and the Tax administration to their platform. This means Mercell's clients cannot access data from the additional sources available in the service. Due to the late implementation of eBevis into Artifik's tender platform we were unable to use eBevis as a part of this pilot.

Another limitation to eBevis is that the process of collecting data has to be repeated for every tender, even if the same CA and EO are involved in two separate tenders at the same time. In contrast a tax certificate in PDF is valid for six months in Norway.

eBevis only collects data from selected public sources, but there are many non-public evidence sources widely used in Norwegian public procurement such as The Eco-Lighthouse Foundation. All data sources not included in eBevis are still shared as PDF.

The public procurement use case is aiming to solve the following challenges[1][2][3]:

- High transaction costs for public procurement processes, estimated to 4,1 % of contract value
- Labour marked crime and labour exploitation
- Reduced transparency and accountability in public procurement

[1] "Rapport til anskaffelsesutvalget: Offentlige anskaffelser 2022» by Oslo Economics and Inventura, a report in Norwegian describing the transactional cost of public procurement - https://osloeconomics.no/wp-content/uploads/2023/11/OE-rapport-2023-51.-Rapport-til-anskaffelsesutvalget.-Offentlige-anskaffelser-i-2022.pdf

[2] "Special report 28/2023 – Public procurement in the EU" by the European Court of Auditors - https://www.eca.europa.eu/en/publications?ref=sr-2023-28

[3] "Action plan to combat social dumping and work-related crime" by the Norwegian government. - https://www.regjeringen.no/en/dokumenter/Action-plan-to-combat-social-dumping-and-work-related-crime/id2928944

- Cross-border, eCertis

This use case proposes the following improvements in solving the challenges:

- Reduce transaction cost for both Economic Operators (EOs) and Contracting Authorities (CAs). Time spent collecting, sharing, requesting and verifying evidence will be significantly cut for both parties using wallet technology.
- Wallet technology can provide authentic data that cannot be altered, this will reduce labour market crime and labour exploitation.
- To increase transparency and accountability we need a completely digitalized public procurement process. Moving from evidences in PDF format to digital evidences based on wallet technology is an important step to digitally transform the public procurement process. Wallet technology is scalable, unlike eBevis, and new data sources (public and non-public) can be added and made available to the users *without the potential bottle neck of the tender platforms*. Wallet technology is also available to both public and private Contracting Authorities, creating a common best practice for all businesses.

3.1.3 Business process overview and value

The business process in the current state of things without the wallet (not using eBevis):

1. EO logs in to Altinn to download a tax certificate in PDF every six months. A new business certificate has to be downloaded in PDF every time there are changes to the board, the company address etc. Depending on the criteria set by the CA other evidence must also be collected, usually in PDF.
2. When replying to a tender, the PDFs of requested selection criteria must be uploaded to the tender platform together with the tender documents.
3. When opening the tender, the CA must evaluate the evidences in PDF and verify if they are up to date and genuine.
4. During the contracting period, the CA must manually request updated documentation of requested criteria from the EO if they have a contractual obligation to be valid throughout the period.

In the future with the wallet ecosystem:

1. EO creates a company wallet, imports and stores LPID and verified credentials from relevant data providers. The credentials are collected once and can be shared with multiple CAs.
2. When replying to a tender, the EO connects their company wallet with the tender portal and shares requested verified credential with the CA together with the bid documents.
3. The CA can view the verified credentials in the tender portal together with the bid documents. They can trust that the credentials are genuine and do not need additional control mechanisms.
4. Ideally, the possibility of monitoring evidences will also be in place, so that EOs and CAs can be notified in case a credential is no longer valid.
5. The wallet gives the users an overview of all credentials that they have shared with others or is shared with them.

Figure 1 shows a high-level overview of the above. For this use case, we assume that economic operators and contracting authorities will access the wallet and verified credentials via an enterprise software such as a tender platform.

Co-funded by
the European Union

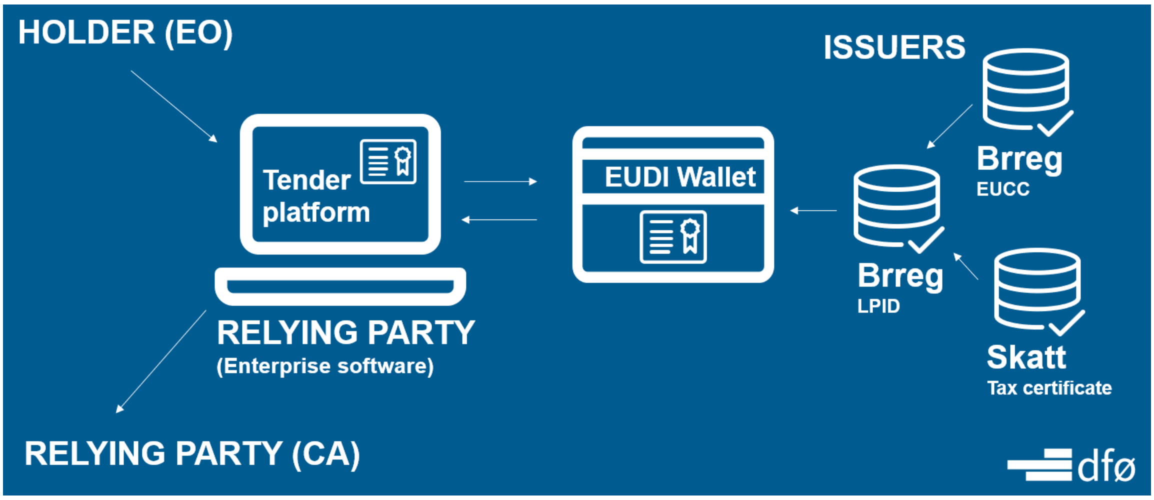


Figure 1 High-level overview

The overall business value is a simplified public procurement process, resulting in better spending of public funds.

- **Business growth:** Easier to participate in public procurement processes, can expand business opportunities for smaller businesses and the innovation rate for public organizations. Many suppliers find the workload of public procurement too big and avoid replying to tenders, particularly start-ups. Using wallet technology can also improve cross-border procurement, making it easier for both EOs and CAs to apply for and accept foreign business partners. This could have a major impact on the EU's economy, as public procurement already represents around 14 % of the EUs GDP, which translates to roughly €2 trillion annually.
- **Time saved and reduction of administrative burden:** Collecting and verifying credentials take a lot of time for both EOs and CAs today. Administering credentials requires time that could be used on creating actual value, such as writing quality bids that meet the client's needs, and evaluating tenders that best fit the request.
- **Fraud prevention:** The wallet technology can provide verified credentials, eliminating the need for CAs to validate documentation in PDF. This will reduce fraud, labour market crime and labour exploitation.

The direct business value of this pilot is a proof of concept, showing that the data flow of sharing validated credentials from an EO to a CA, via a tender platform, using a wallet in a public procurement process works. This can be developed further in new pilots with added complexity such as additional data sources, combining wallet with the European Single Procurement Document (ESPD), cross-border procurement, different wallet providers and additional tender platforms.

3.1.4 Architecture and infrastructure

Figure 2 shows the pilot architecture of the procurement process using a wallet.

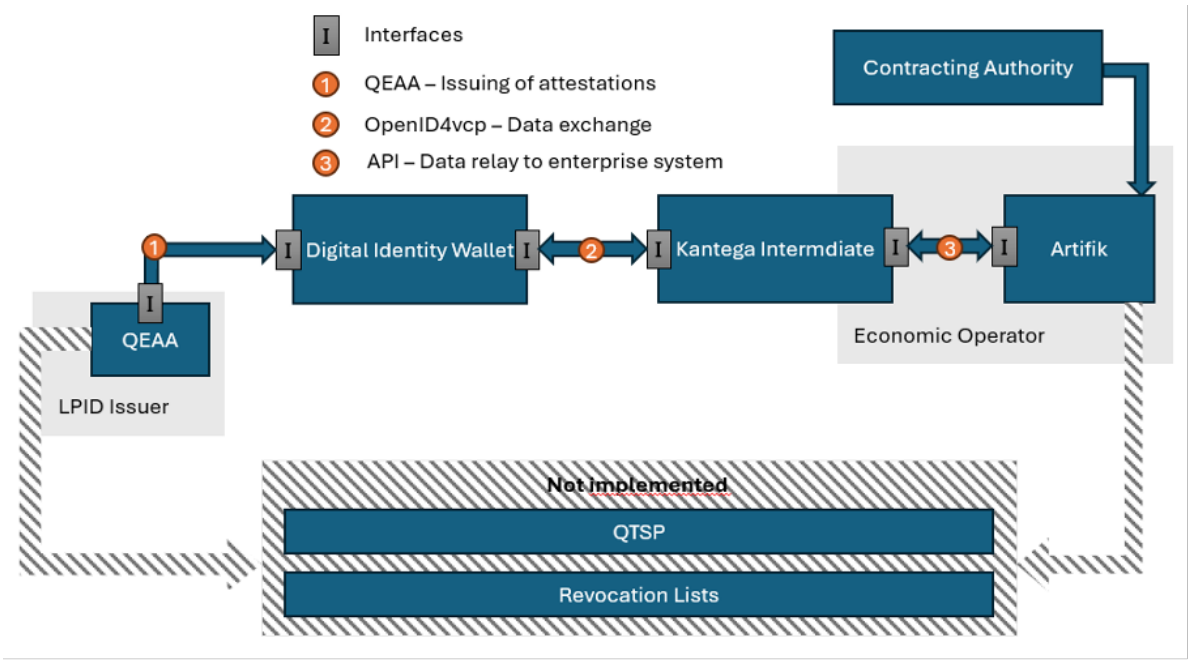


Figure 2 Architecture and topology

Roles:

EUDIW: iGrant.io

PUB-EAA issuer (QTSP): Brønnøysundregistrene

Relying party: Artifik (tender platform) as data user

Intermediate: Kantega (temporary evidence service as Relying Party)

Holder: EO

End user: CA

When the EO clicks the link/button in Artifik to collect attestation via wallet, an API call is sent from Artifik to Kantega. Kantega then creates a presentation request that is served to the EO through Artifik. The EO accepts the credential presentation request in the wallet application (iGrant) and data is then shared through Kantega as an intermediate to Artifik. The CA can then view the presented attestation as part of their evaluation process in Artifik.

3.2 P1.1.2 Automated verification of Economic Operator identity in the procurement process flow (ESPD)

3.2.1 Pilot description

The pilot focuses on the authentication and verification of an Economic Operator (EO) identity in an ESPD (European Single Procurement Document) service as part of a cross-border public procurement process. Once authenticated, the EO uses their company EUDIW to present the required company data, which automatically populate the corresponding ESPD form fields, reducing administrative burdens and streamlining participation for businesses.

EWC partners involved:

- UPRC: Technological partner - developer of ESPD service

Co-funded by the European Union

- Netsmart/Telesto technologies: Technological partners
- Finnish Tax Authority (Vero): provided Mini-DVV as test issuer and Mini-Wallet as test company wallet
- Direktoratet for Forvaltning og Økonomistyring (DFO): The Norwegian Agency for Public and Financial Management
- Brønnøysundregistrene: Norwegian Business Registry - Issuer
- iGrant: wallet provider

The pilot showcases how EUDIW can be used by organizations to authenticate themselves to an ESPD service as part of a cross-border procurement process. The pilot begins with pre-issued attestations already available in both an individual wallet and a company wallet, as is the establishment of trust frameworks for credential issuance. Additionally, since no LoA high mechanisms are currently available, any verification processes requiring LoA high are also considered out of scope.

The **motivation and goals of the pilot** are the following:

1. How companies and their legal representative authenticate to an ESPD service.
2. How company data can be shared and presented to an ESPD service securely and with a user-friendly way, using the EUDIW.

The main goal is to simplify the use of an ESPD service by companies during their bidding preparation within a procurement process and help companies expand their business (participate in more public procurement processes), lower administrative burden on companies, and prevent fraud by verifying company identity.

3.2.2 State-of-the-art (SOTA) analysis

EU public procurement is regulated by the 2014 Procurement Directives (2014/24/EU[4] , 2014/25/EU[5]) which establish a common legal framework aiming to ensure open, transparent, and competitive tendering procedures across all Member States. Even though the legal framework offers common rules, their implementation and digital maturity vary significantly between countries.

Most EU countries now operate national eProcurement platforms to manage the tendering process and support digital submission of bids. These include platforms such as TED (Tenders Electronic Daily) at the EU level, and national systems like NEPPS in Greece. All EU countries are also required to support the ESPD, intended to simplify declarations regarding exclusion and selection criteria.

In Greece, the National eProcurement System[6] (NEPPS - ΕΣΗΔΗΣ) is the main online digital platform for public procurement. It is complemented by the Central Electronic Public Procurement Registry (CEPPR - ΚΗΜΔΗΣ) which ensures transparency by collecting and publishing all information concerning public procurement and contracts. Promitheus, offered by NEPPS functions as the Greek national ESPD Service, allowing Contracting Authorities and Economic Operators to prepare and submit ESPD requests and responses electronically.

[4] European Union. (2014). Directive 2014/24/EU - https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng

[5] European Union. (2014). Directive 2014/25/EU - https://eur-lex.europa.eu/eli/dir/2014/25/oj/eng

[6] National Electronic Public Procurement System - Online platform promitheus.gov.gr

Despite these developments, current systems across EU countries remain heavily reliant on manual processes. Identity and company information must often be entered manually and supported documents are typically uploaded as PDF files. Key functions such as identity verification and company validation continue to be based on scanned PDF documents, lacking automatic validation mechanisms.

EOs that seek to participate in public tenders face the following technical and administrative challenges:

- **Manual processes:**
  - EOs must enter identity and company data into national systems repeatedly
  - Forms are populated manually, which can introduce errors
- **Use of unstructured documents**
  - Supporting evidence (e.g., company registration) is typically uploaded as a scanned PDF documents
  - Scanned PDF documents are not machine-readable, which require time consuming manual verification from Contracting Authorities (CAs).
- **Non interoperable systems**
  - Verification of company and representative details often depends on national registries, which are not interoperable across borders
- **Lack of standardization**
  - Supporting documents are rarely standardized
  - National procurement procedures may differ, even when operating under common EU rules

These challenges increase the administrative burden on businesses and discourage participation in public tenders. This in turn limits competition and reduces business opportunities. The Special Report 28/2023[7] of the European Court of Auditors (ECA) highlights these trends noting that the single-bid tenders across the EU rose from 23,5% in 2011 to 41.8% in 2021, which is a clear indication of decline in competition in public procurement. Additionally, SMEs, continue to face challenges in accessing public procurement opportunities especially across borders. These include complex documentation requirements, lack of transparency, and limited digital support all of which contribute to low participation rates despite SMEs representing over 99% of EU businesses (Stratford Journals, 2023[8]).

The piloted use case serves as a proof of concept on how the integration of the EUDI wallet into the public procurement process can significantly reduce administrative burden, improve trust and facilitate cross-border participation. By using verifiable credentials that are structured (machine readable), authentic and up to date (retrieved directly from trusted authorities) trusted interactions across borders can be enabled without reliance on repetitive manual data entry, scanned PDFs and fragmented national verification systems.

3.2.3 Business process overview and value

Generally, the main actors and roles involved in an ESPD process are the following:

[7] European Court of Auditors (2023). Special Report 28/2023 https://www.eca.europa.eu/en/publications/SR-2023-28

[8] Stratford Journals. (2023). Challenges Faced by SMEs in Public Procurement within the European Union. Journal of Procurement & Supply Chain, 7(1) - https://www.stratfordjournals.com/journals/index.php/journal-of-procurement-supply/article/view/2384/3024

- **Contracting Authority (CA):** public entity responsible for conducting the public procurement procedure. The CA defines criteria to be fulfilled by bidding EOs, evaluates the submitted evidence and eventually awards the procurement contract. The CA sets the award criteria by generating an ESPD request.
- **Economic Operator (EO):** business entity that participates in a public procurement procedure and fills the ESPD form as part of their bid submission. The EO imports an ESPD request and generates an ESPD response, stating their compliance with the criteria defined by the CA in the request.
- **Regulatory body:** entity that governs the procurement process (Greek Ministry of Digital Governance - MDG)

Note: The ESPD request creation is out of scope. The pilot begins by importing an already established ESPD request and initiating the ESPD response filling process.

In the context of the **EWC Pilot**:

- **Issuer:** Business Register that issues LPID, EUCC to company wallet holders and acts as the authentic source.
- **Wallet holder:** End users acting on behalf of an EO (Legal Representative).
- **Relying party:** National ESPD service that the EO uses to create their ESPD response.

Typical steps that an EO follows to submit an ESPD response in a public procurement process without the wallet.

Note: The EO has already downloaded the ESPD request created by the CA prior to initiating the ESPD response process.

1. **Access Procurement Platform:** The EO accesses the national procurement portal (Promitheus in Greece)
2. **ESPD request import:** The EO imports the ESPD Request issued by the CA and reviews the exclusion and selection criteria.
3. **Manual Data Entry:** The EO manually fills in the ESPD Response form. Company details (name, registration number, address etc.) and legal representative information are all required by the ESPD and entered manually.
4. **Attach supporting Documents:** The EO attached required evidence (tax clearance, company registration etc.) as scanned PDFs or other unstructured documents. These documents need to be translated and validated separately.
5. **Submission:** The EO includes the ESPD response to their bid and submits it.
6. **Contracting Authority review:** The Contracting Authority performs manual verification of submitted documents and company details, which significantly introduces delays to the evaluation process.

The following section outlines the process enabled by the EUDI wallet ecosystem:

Note: The EO has already downloaded the ESPD request created by the CA prior to initiating the ESPD response process.

1. **Access Procurement Platform:** The EO accesses the national procurement portal (Promitheus in Greece)
2. **ESPD request import:** The EO imports the ESPD Request issued by the CA and reviews the exclusion and selection criteria.
3. **Present Verifiable Credentials:** The EO uses the EUDI wallet to present necessary verifiable credentials:

Co-funded by
the European Union

   a. NPID (Natural Person Identifier) for identity of legal representative
   b. LPID (Legal Person Identifier) and
   c. EUCC (EU Company Certificate) for company details.

   The credentials are retrieved from trusted issuers, are machine-readable and verified instantly by the ESPD Service. The ESPD form is auto filled using verified data from the credentials.

4. **Submission:** The EO includes the ESPD response to their bid and submits it.
5. **Contracting Authority review:** The Contracting Authority can instantly trust and process the data without additional manual checks.

The pilot envisions to show how the integration of the EUDI Wallet into the public procurement processes can transform the way businesses (especially SMEs) can interact with public sector platforms across the EU. The business value of this use case is allowing companies to participate in public tenders more efficiently, without repeatedly submitting paper-based or scanned documents. EU businesses will benefit from faster application processes, fewer error and lower administrative costs, which in turn results in new opportunities for businesses of all sizes across all EU countries.

3.2.4 Architecture and infrastructure

The pilot was conducted in **two iterations**.

1st iteration

The first iteration ran during Phase 2 of EWC and was completed in May 2025. It was demonstrated in EWC General Assembly held in Stockholm in May. Figure 3 illustrates the architecture used in this iteration. In that iteration, attestations (LPID, EUCC and NPID) were issued by Mini-DVV test issuer of the Finnish Tax Administration (Vero). The company wallet used was the Mini-Wallet, while the personal wallet used was iGrant's mobile data wallet app. The Greek ESPD Service Promitheus acted as the Relying Party. QTSP was out of scope and not used.

A video of the demo presented at the Stockholm GA is available at: https://nextcloud.ewc-consortium.eu/s/Pz6cFcS9tKknDbe

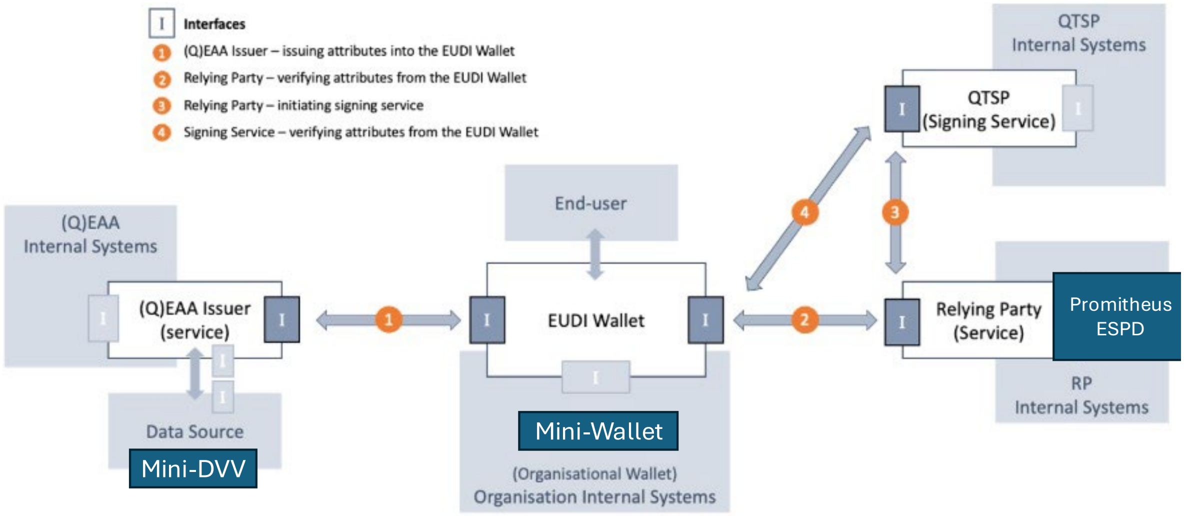

I Interfaces
1 (Q)EAA Issuer – issuing attributes into the EUDI Wallet
2 Relying Party – verifying attributes from the EUDI Wallet
3 Relying Party – initiating signing service
4 Signing Service – verifying attributes from the EUDI Wallet
QTSP Internal Systems
QTSP (Signing Service)
End-user
(Q)EAA Internal Systems
(Q)EAA Issuer (service)
EUDI Wallet
Relying Party (Service)
Promitheus ESPD
RP Internal Systems
Data Source
Mini-DVV
Mini-Wallet
(Organisational Wallet)
Organisation Internal Systems
I
1
2
3
4

Figure 3 Overview diagram of 1st iteration of public procurement pilot

2nd iteration

The second iteration, shown in Figure 4, was completed in July 2025. In this iteration, Brønnøysundregistrene and DFO joined by issuing the LPID, EUCC and NPID attestations. The company wallet used was iGrant's Dev Enterprise wallet, and the personal wallet used was iGrant's data wallet mobile app. The Greek ESPD Service Promitheus acted again as the Relying Party.

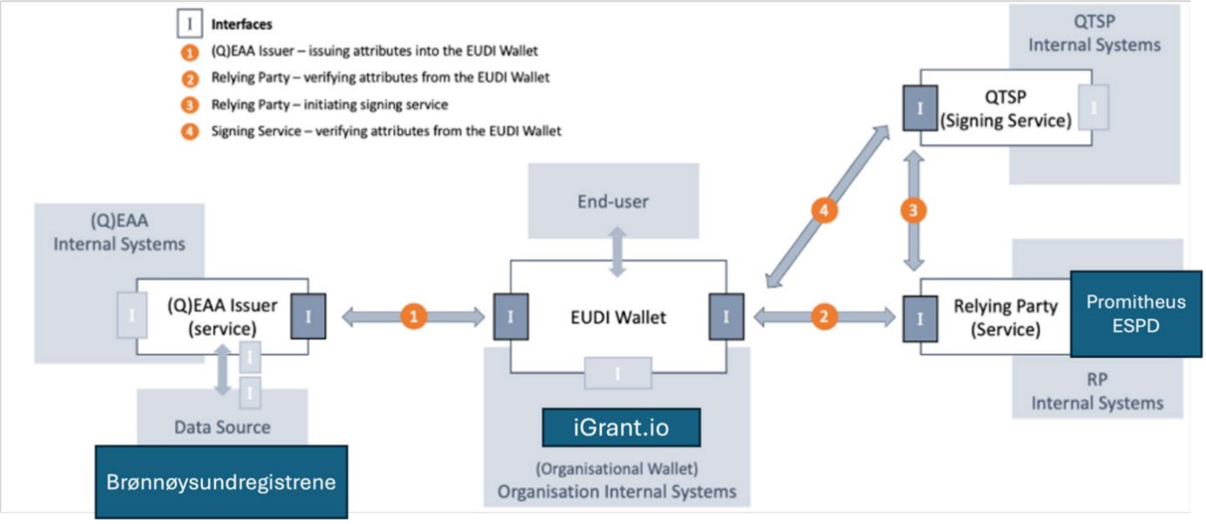

I Interfaces
1 (Q)EAA Issuer – issuing attributes into the EUDI Wallet
2 Relying Party – verifying attributes from the EUDI Wallet
3 Relying Party – initiating signing service
4 Signing Service – verifying attributes from the EUDI Wallet
QTSP Internal Systems
QTSP (Signing Service)
End-user
(Q)EAA Internal Systems
(Q)EAA Issuer (service)
EUDI Wallet
Relying Party (Service)
Promitheus ESPD
RP Internal Systems
Data Source
Brønnøysundregistrene
iGrant.io
(Organisational Wallet)
Organisation Internal Systems

Figure 4 overview diagram of 2nd iteration of public procurement pilot

The pilot steps are presented below in greater detail:

1. **Accessing the ESPD service:** The Legal representative of EO navigates to and accesses the national ESPD service via a website URL.
2. **Authentication with Individual digital wallet:** The EO Legal representative is authenticated to the ESPD service by scanning a QR code that represents a OID4VP NPID presentation request created by the ESPD Service.
3. **Verification of identity:** The ESPD service verifies the identity of the Legal Representative.
4. **Import of ESPD request:** Following successful authentication, the EO legal representative imports an ESPD request and initiates the ESPD response form fulfilment.
5. **Legal representative provides company's wallet eAddress or openIdOrganisationId to the ESPD service[9]:** The Legal Representative provides the company's wallet eAddress or openIdOrganisationId to the ESPD service by filling a form field.
6. **Company data presentation:** The ESPD Service makes LPID and EUCC presentation requests to the company's wallet using the eAddress or openIdOrganisationId provided in the previous step. The EO presents company data required by the ESPD form.
7. **Company data presentation:** The company wallet responds with the LPID and EUCC data.

[9] Note: The first iteration of the pilot supported eAddress as the mechanism for invoking the company wallet. However, since eAddress is not standardized, it was replaced with openIdOrganizationId in the second iteration.

8. **ESPD Service verifies LPID and EUCC data:** ESPD Service cross-checks and verifies LPID and EUCC data. If verified, then automatically populates the EO related ESPD form fields.
9. **ESPD response generation:** The EO legal representative proceeds on replying to the qualification criteria set by the CA and generate their ESPD response (download the ESPD response XML file)**.**

A sequence diagram and general architecture interaction's diagram are presented in Figure 5 and Figure 6, respectively to illustrate the steps described above.

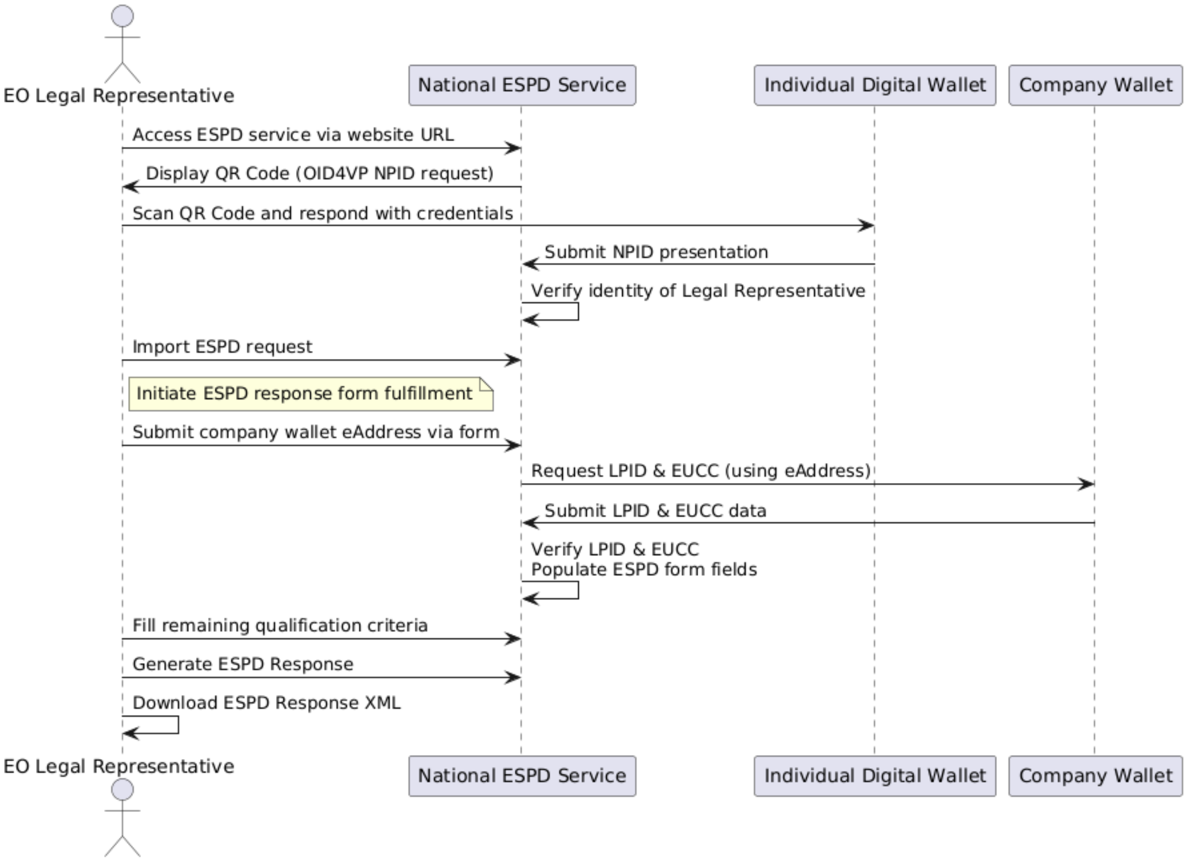

EO Legal Representative
National ESPD Service
Individual Digital Wallet
Company Wallet
Access ESPD service via website URL
Display QR Code (OID4VP NPID request)
Scan QR Code and respond with credentials
Submit NPID presentation
Verify identity of Legal Representative
Import ESPD request
Initiate ESPD response form fulfillment
Submit company wallet eAddress via form
Request LPID & EUCC (using eAddress)
Submit LPID & EUCC data
Verify LPID & EUCC
Populate ESPD form fields
Fill remaining qualification criteria
Generate ESPD Response
Download ESPD Response XML
EO Legal Representative
National ESPD Service
Individual Digital Wallet
Company Wallet

Figure 5 EO authentication to ESPD service pilot steps

Figure 6 presents a high-level interaction's overview with colour coded flows for each technical component of the pilot.

Co-funded by
the European Union

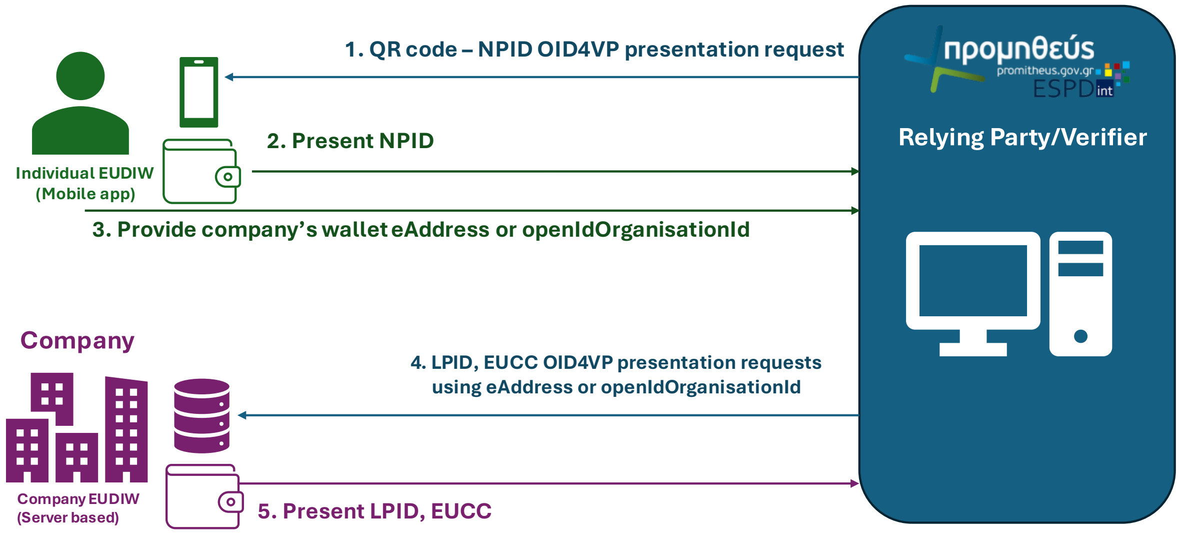

1. QR code – NPID OID4VP presentation request
προμηθεύς
promitheus.gov.gr
ESPD int
Relying Party/Verifier
Individual EUDIW
(Mobile app)
2. Present NPID
3. Provide company's wallet eAddress or openIdOrganisationId
Company
4. LPID, EUCC OID4VP presentation requests
using eAddress or openIdOrganisationId
Company EUDIW
(Server based)
5. Present LPID, EUCC

Figure 6 High-level interaction's overview diagram

3.3 P2.1.1 Onboarding new Business Partner

3.3.1 Pilot description

The KYS business scenario (Onboarding a new business partner) focuses on a basic B2B use case with an exchange of documents between two companies doing business together. This business scenario implicates a client which needs to verify his new supplier's conformity through a verification process that is highly subject to fraud.

EWC partners involved:

- Infogreffe as LPID + PUB-EAA provider
- Powens / ID360 as RVP (inside Archipels wallet)
- Archipels as Wallet provider
- French Clerks of the commercial court, KVK as Authentic sources
- Archipels as Trust list provider
- Legallais, S.O.R.I.B.A, Coopérative vendéenne du logement, ETS LIBAUD, Newtech Interactive, Medialex, Jifmar Offshore service as Relying parties
- SASU Jonathan Bonnet, ZenCFO, Jideca, Eliness, Besigaki, N2J immobilier as Suppliers (Holder)

This **pilot aimed** to demonstrate that the wallet can secure, facilitate and automate KYS process.

The pilot main hypothesis is that: The Legal EUDIW can be used for an automated onboarding process of a partner by another organization where we will conduct the verification of the identity of the person representing the company and the legal identity of the company. The process will be managed via a Legal Person wallet from both parties:

- A Legal Person wallet can create a connection with another wallet
- A Legal Person wallet can request attestations to authentic sources through the wallet
- A Legal Person wallet can request to another wallet to present attestations (Organizational credentials)
- A Legal Person wallet can present attestations to a relying party
- A Legal Person wallet can "transfer" attestations to an internal system

This was tested initially between a company with its suppliers within its own country (France) and the plan was to perform a cross-border exchange of attestations between two European (French and Dutch) organizations enrolled within the help of business registries from EWC, but at the end this did not materialise due to Archiples early exit from the project.

The 2nd hypothesis concerning the facilitation of onboarding through legal documents signing in addition to the automation of KYS documents exchange presented in D3.5, has not been conducted because of a lack of advancement in the development of this functionality.

The **motivation and goals of the pilot** are the following:

Using the EUDI wallet, the business process can be nearly completely automated (exception is the identification step) at least for those business partners who own an interoperable EUDI Wallet.

Instead of maintaining up to several millions (for big companies) of master data sets the data are issued by (Q)EAA Providers, requested as verifiable attestation presentations from the business partner, automatically verified and transferred to internal IT systems. Therefore, significant master data maintenance costs can be saved and process quality costs in payment, logistics and manufacturing processes caused by wrong master data can be avoided.

Business objectives and benefits:

- Reduce the master data maintenance costs by significantly reducing the number of “golden record” data sets stored by all legal entities. Today each company stores and maintains the data of all other companies. In a steady state where all the business partners have interoperable organizational wallets the existing master data management costs of a legal entity can be reduced by a factor that equals the number of business partners. Let’s consider the following example:

So, if we consider 10 companies which each have a relationship with each other, each company has to store and to maintain 10 master data sets. The maintenance costs per public master dataset (name, address, bank accounts, VAT Nr....) and per year were calculated by the German Verband Deutscher Automobilhersteller (VDA) in 2022 to 11 EUR/year and business partner. So, each company must spend 110 EUR for business master data maintenance.

By using the Legal EUDIW and the automated data transfer process the costs can be reduced by the factor 10 to approx. 11 EUR, the cost for the own master data set maintenance. Big companies must maintain several millions of business partner master data sets. So, the cost savings are significant. New additional costs occur due to the need to pay for the own (Q)EAA’s that contain master data relevant attributes and Legal EUDIW operating costs. These costs however are not use case specific, because these data and the wallet are use case agnostic and can be used in several use cases form different business processes.

- Reduce logistics and finance process quality costs due to insufficient master data quality (e.g.: diminish bank account fraud activities)
- Increase the quality of the business partner master data sets by increasing actuality and by completely removing human manual data entries in legal entities. The data source are issuer data bases (bank account data) or registries (e.g., commercial registry).
- Reduce the onboarding time of new suppliers:
- Reduce the complexity of verifying identities and information when many actors are involved.

- Remove the need for paper and data that is not machine-readable. Enables more fully digital processes and time efficiency with automated processes.
- Increase traceability and security on information handling and data exchange between legal entities.
- Deliver required proofs and certificates in seconds with reduced lead times as a result at lower operating cost.
- Make cross-border trade easier since interoperability is ensured with the wallet solution and trust can be established through automatic validation and verification of information that is law-abiding.

Functional goals:

The business scenario KYS aims to demonstrate the ability of two organisations to exchange efficiently their LPID to establish a trusted connection between them and then present a set of organisation attestations requested in case of a partner onboarding. We looked for different types of organizations to participate:

- a company A (client) with a company B (supplier) from the same country
- a company A and company B from two different countries
- a company A (large enterprise) and a set of companies B (SMEs) from the same country
- a company A (large enterprise) and a set of companies B from different countries

It was expected that not all the company invited would accept to participate to all the steps.

Performance goals:

- The highest conversion rate of companies engaged to execute the functions suggested in the KYS pilot and to perform it among the suggested types of organizations listed.
- The number of companies to execute it successfully to contribute to our overall EWC KPIs of Legal wallet usage.

Quality Goals:

- Reduce the master data maintenance costs.
- Increase the quality of the business partner master data sets.
- Reduce the onboarding time of new suppliers.

3.3.2 State-of-the-art (SOTA) analysis

Archipels ceased its operations and exited EWC early 2025, and not all sections of D3.6 are completed.

3.3.3 Business process overview and value

The KYS business scenario starts with a Legal person wallet already validated (according to RFC 005 for LPID issuance protocol).

We defined few steps to test this scenario:

- Step 1: The Legal wallet of the client will send a presentation request to the supplier. This request can be sent by email taking into consideration that the supplier doesn't have a wallet at this stage.
- Step 2: Presentation of mandatory LPID attestation to establish the trust.

- Step 3: Presentation by the supplier of its LPID, EUCC, IBAN attestation. This will require that an IBAN attestation is issued by a QEAA provider, and the company wallet is able to request it, store it and present it on demand.
- Step 4: Enable companies to transfer the data presented to company IT system for reconciliation and maintain a master data set.

Note: In the national phase that took place before the Organizational attestations' standard availability, national attestations, defined with the help of the French business registry: KBIS and IBAN. Figure 7 shows a recap of the business process. For this use case, we assume that Economic Operators and Contracting Authorities will access the wallet and verified credentials via an enterprise software such as a tender platform.

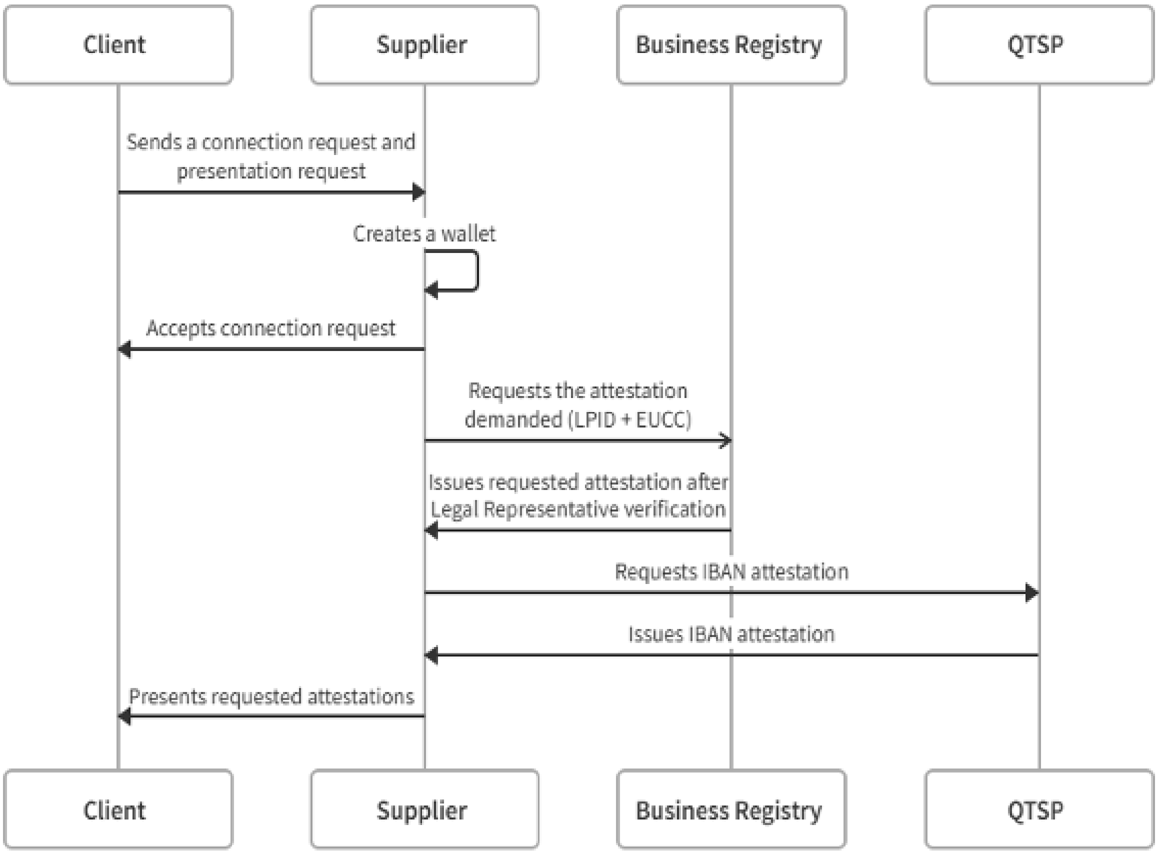

Client
Supplier
Business Registry
QTSP
Sends a connection request and presentation request
Creates a wallet
Accepts connection request
Requests the attestation demanded (LPID + EUCC)
Issues requested attestation after Legal Representative verification
Requests IBAN attestation
Issues IBAN attestation
Presents requested attestations
Client
Supplier
Business Registry
QTSP

Figure 7 KYS process recap

3.3.4 Architecture and infrastructure

Figure 8 shows an overview diagram of the KYS pilot topology.

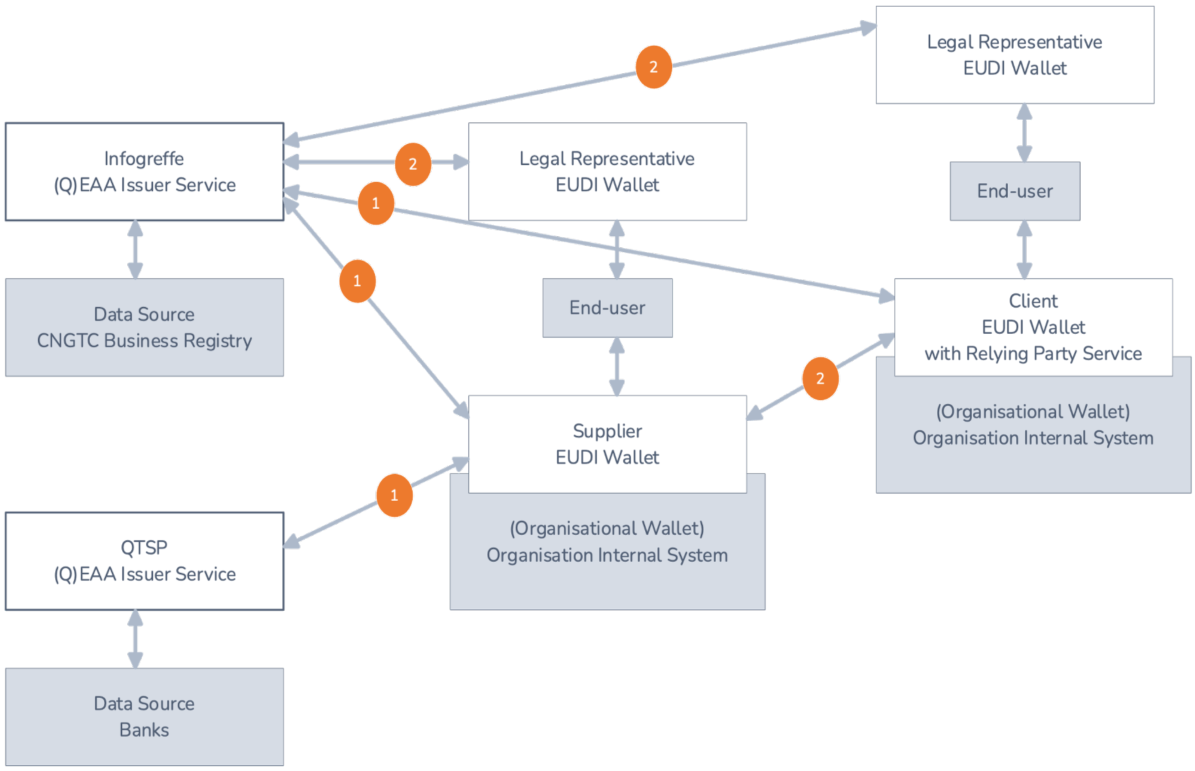

Legal Representative EUDI Wallet
Infogreffe (Q)EAA Issuer Service
Legal Representative EUDI Wallet
End-user
Data Source CNGTC Business Registry
End-user
Client EUDI Wallet with Relying Party Service
(Organisational Wallet) Organisation Internal System
Supplier EUDI Wallet
(Organisational Wallet) Organisation Internal System
QTSP (Q)EAA Issuer Service
Data Source Banks
1
2

Figure 8 KYS overview diagram of architecture and topology

The implementation of the business flow is structured around three key roles within the ecosystem:

1. **Issuers**

- Infogreffe: As the manager of the French Business Registry, Infogreffe issues KBIS, LPID, and EUCC attestations.
- Qualified Trust Service Provider (QTSP): Connected to multiple banking institutions to issue IBAN attestations.

2. **Organizational wallets**

- Client Organizations: Entities initiating KYS (Know Your Supplier) processes.
- Supplier Organizations: Entities being onboarded by clients.
- Both primarily function as Relying Parties and Wallet Holders in the verification workflow.

3. **Individual EUDI wallets**

- Utilized by legal representatives of both Clients and Suppliers.
- Essential for identity verification with Infogreffe during the LPID issuance process.

Additional components

- Infogreffe has been enhanced with attribute verification capabilities to streamline the verification pro-cesses required for LPID, KBIS, and EUCC issuance.
- Client organizations also receive LPID attestations to establish their identity with Suppliers, ensuring bidirectional trust in the verification relationship.

The technical evolution was guided by several key considerations:

1. Standards Alignment: Progressive alignment with EWC RFCs to ensure maximum interoperability.

2. Privacy Protection: Maintaining privacy features while transitioning to standardized protocols.
3. Backward Compatibility: Supporting existing implementations while migrating to new standards.
4. Protocol Efficiency: Simplifying the protocol stack by removing unnecessary dependencies.
5. Ecosystem Integration: Ensuring seamless integration with the broader European Wallet Ecosystem.

This phased approach allowed to initiate piloting early and maintain service continuity while evolving the technical implementation to meet the requirements of the EWC standards, particularly EWC-RFC001 for issuance and EWC-RFC002 for verification.

Additional integrations:

- CNGTC Business Registry: Data source connection implementing KBIS, LPID, and EUCC issuance processes per EWC-RFC specifications.
- Banking Institutions: Data source connections for IBAN attestation issuance.
- Internal Systems: Integration with organizational systems via webhooks and access tokens for seamless interaction with organizational wallets.

3.4 P2.2.1 Open a bank account for a business

3.4.1 Pilot description

The pilot idea was to use an EUDIW for organizations to open a bank account for a business in another member state.

EWC partners involved:

The actors in the pilot were the Finnish Tax Administration (Vero), Bosch and KVK who acted in one or several of the roles of a wallet provider, an issuer or a relying party. Findynet co-operative contributed an OpenID Federation server for testing the trust model in the pilot. Mobile wallets provided by wallet providers (iGrant.io, Lissi) in the project were used for natural persons. Spherity and Bundesanzeiger acted as observers of the pilot.

Pilot Scope:

The company's home country's business register issues a business register extract and a beneficiary register extract as (Q)EAAs to the company's wallet. The (Q)EAAs are used for opening a bank account for the company (in the same/different country).

The **motivation and goals of the pilot** are the following:

The Finnish Tax Administration had interviewed two banks in Finland in a previous project. In the interviews, banks have indicated that the Know Your Customer (KYC) process for their business customers causes significant administrational work. Much of the work relates to manual verification of the company evidence. Cross-border KYC for business customers is particularly cumbersome.

The pilot idea was to use an EUDI legal person wallet to open a bank account for a business in another member state. This reduces fraud and cuts costs for the financial institutions without compromising their obligations to know their customers, as defined by the terrorist/anti-money laundry laws (e.g. Directive (EU) 2018/843[10], Regulation (EU) 2024/1624[11]). The pilot further supports the free movement of services in the internal markets by removing obstacles from a cross-border delivery of banking services.

3.4.2 State-of-the-art (SOTA) analysis

Today, a person opening a bank account for a business needs to:

- prove their identity
- demonstrate their right to represent the legal person (present a power or attorney or business register extract indicating them as a signatory)
- provide other necessary evidence, at least the legal person's business register extract, ultimate beneficial owner certificate, articles of association and the latest financial statements

This can be done on paper face-to-face or online using (potentially signed) pdf or other formats. Many banks have also direct access (API) to retrieve the documents from the local business register (but seldom from business registers in other member states).

After collecting the company evidence, the bank needs to verify the evidence and evaluate the risks opening the account may cause under the anti-money laundry (AML) laws. This is expensive manual work for the bank.

According to a study in 2021 (PWC 2021 report "capturing the value of know your customer"), banks spent 21 billion Euro a year in Europe for KYC/AML. For a large bank the cost is 200-400 million Euros a year. The time-consuming and complicated checks cause also frustration for the customers; 54% of clients reported negative experience.

The banks reported difficulties in particular for verifying the evidence for foreign companies, complicating opening a bank account in another member state. This hinders the free movement of banking services in the internal markets.

3.4.3 Business process overview and value

The different steps a user will go through in the current state without the wallet are the following:

Public Authorities issue necessary documents

A legal person needs several documents to open a bank account. Public Authorities, including trade register and tax administration, issue these documents. Public Authorities issue these documents in national language and in paper or pdf formats. There is no generally accepted common structure for these documents. Some tax administrations offer signing for pdf documents to guarantee that documents are not changed during the process. A legal person request these documents manually and shares them manually.

Notarisation and translation

[10] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance)

[11] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance)

In some situation, like opening bank account in another country, a relying party may require a translation of the documents as well as notarisation of the documents. Notarisation is one way to secure authenticity of the document. When a bank is not in the same country where a legal person is registered, the bank may lack solutions to verify the documents, and therefore notarisation is required.

Process at the bank

When there is no common structure for the documents and they are in pdf format, the bank must handle documents in many cases manually. When a KYC procedure is obligatory for the bank, the possibility to use scanners and other tools for text processing may be restricted, because a mistake in interpretation of the documents may result losses and liabilities. When a legal person opens a bank account in another country, it is common to require physical presence during which the passport is controlled, so that the bank has identified in person the authorized person. Depending on the case the bank decides how often the documents must be updated and verified. For this verification a legal person has to request and share some of documents to indicate status at the point of verification. If a legal person does not submit valid documents, the bank may close or freeze the account.

By using the EUDI wallet we seek for a faster automated KYC/AML process in a bank without sacrificing the integrity and security of the process. The EU-wide data models for the related attestations also simplify opening a bank account in another member state, supporting the free movement of banking services.

This section describes the business process implemented in the pilot. The legal person representative uses their natural person EUDIW to log in to an on-line bank abroad. They then identify the legal person's EUDIW which the bank uses for authenticating the legal person and retrieving its EU company certificate (Directive (EU) 2025/25 article 16b). The bank then uses the EU company certificate to verify the natural person is a legal representative of the company. If that cannot be done, the bank can request the natural person to present from an EUDIW a separate Power of Attorney, indicating their authorization to act on behalf of the legal person.

The piloted business process ended when the bank had received these attestations from the users. Also, necessary but out-of-scope for the pilot was an attestation on the legal person's ultimate beneficial owners, articles of association and latest financial statement. These attestations can be issued to the wallet (depending on national practices, e.g. by the business register) and presented to the bank when their data models are finished. Signing a bank account contract was also out of scope but could be done using the legal representative's EUDIW.

<u>Business Value:</u>

After implementing the pilot, we demonstrated the pilot system to a KYC expert of Landesbank Baden-Württemberg, a German publicly owned bank that collaborates closely with Bundesanzeiger, the German business register. We asked him to reflect his impressions and views on the pilot.

In his opinion, the piloted approach could potentially evolve into something that literally aligns with the term “digitalization” – with far-reaching and profound changes in processes, roles, and divisions of labour. Above all, it could offer a way to technologically counter or even eliminate non-value-adding activities in a bank. It could also lead to entirely new forms of collaboration and potentially new business opportunities – especially for and with those who have high standards to meet.

Co-funded by
the European Union

In 2024, the EU adopted the EU AML regulation (2024/1624), which will be applicable across Europe starting mid-2027. It also addresses customer due diligence obligations and how these are to be fulfilled. Articles 22 and 62 of the regulation cover the identification requirements for natural and legal persons. The Landesbank Baden-Württemberg representative believes the pilot should serve as a forward-looking reference point when it comes to the required information for proper identification, the permissible sources and procedures, and the required trust levels.

The regulation not only outlines what obliged entities must do but also addresses the cooperation obligations of customers. It appears the customers are expected to provide significantly more than what is currently standard practice. This offers a good opportunity for the approach adopted in the pilot.

3.4.4 Architecture and infrastructure

Figure 9 depicts the high-level architecture described below. In the upper part of Figure 9 is the natural person (legal person representative), who uses their natural person wallet to log in to an on-line bank. To do that, they present to the bank a natural person identification data (natural PID) that a PID issuer has issued to their EUDIW. Once logged in, they initiate opening a bank account for a business and identify the EUDIW of the legal person.

In the lower part of Figure 9, the legal person has a server-based wallet to which it has received a legal person identification data (legal PID) and EU company certificate from a competent issuer. The bank requests the Legal PID and EU company certificate from the legal person EUDIW which presents them to the bank. If necessary, they can be complemented by a Power of Attorney attestation (potentially issued by the business register, a QTSP or the company itself, if applicable).

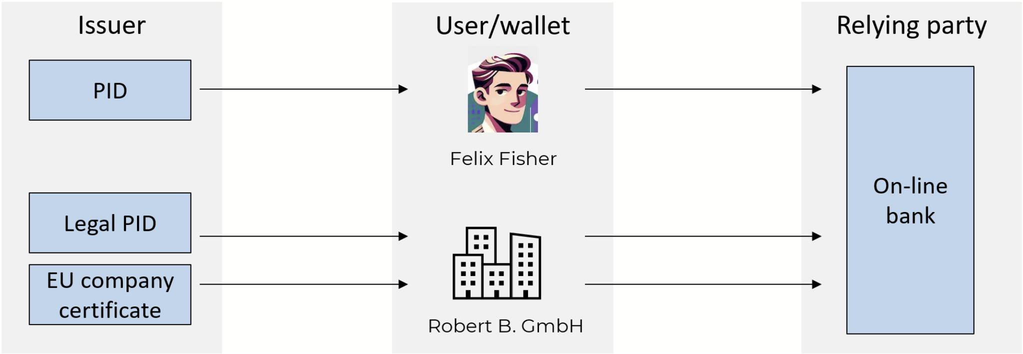


Figure 9 High-level architecture of KYC opening a bank account

The pilot was implemented in three iterations which are clarified in Figure 10. All iterations made use of fictive natural and legal persons and a test bank.

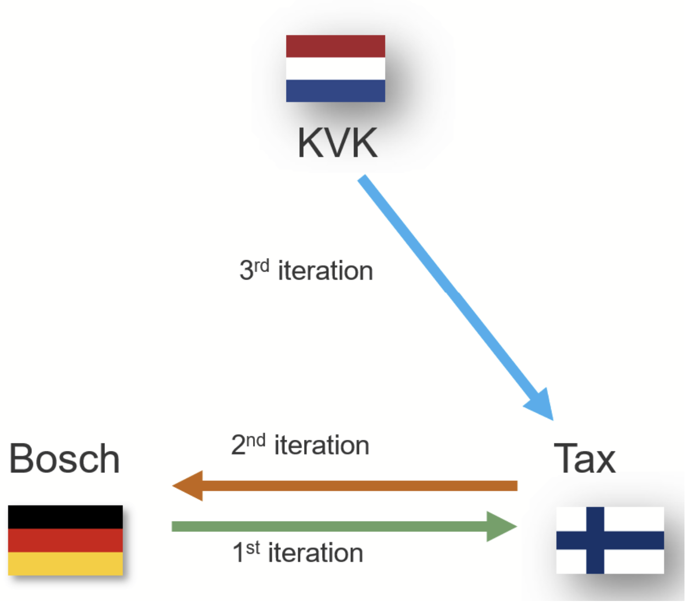


Figure 10 Open bank account iterations

1st iteration

The first iteration was completed in September 2024 and demonstrated in EWC GA in Madrid in October 2024. In that iteration the attestations (legal PID and EU company certificate) were issued and the legal person's server wallet provided by Bosch and the relying party (bank) by the Finnish Tax Administration. The PID issuer in the EWC Phase 1 pilot (University of Aegean) issued the natural PID to the user's mobile wallet (iGrant.io Data wallet). A public screencast video on 1st iteration: https://www.youtube.com/watch?v=XxAt9MyYfLg. A full report on the first iteration is available here

2nd iteration

The second iteration was completed and demonstrated in December 2024. In that iteration, the issuer of the natural and legal PID and the EU company certificate attestations was the Mini-Suomi test environment of the Finnish Tax Administration. Mini-Suomi's Mini-Wallet was used as the server-based wallet for the legal person and Lissi as the natural person's mobile wallet. The relying party (bank) was provided by Bosch. As new functionality, the 2nd iteration provided:

- Optional Power of Attorney attestation that the natural person can present to the bank to demonstrate they are a competent representative despite not listed in the EU company certificate. The issuer of the Power of Attorney attestation was the company itself, and it could be issued either to the legal person wallet or its representative's natural person wallet.
- OpenID Federation based trust evaluation. The relying party accepted only attestations issued by an issuer that had a valid entity statement in the OpenID Federation server (see next section for details).

Project internal recording on the demo of the 2nd iteration: https://nextcloud.ewc-consortium.eu/s/xkZfZZL5MzfQRof . A full report on the 2nd iteration is available here.

3rd iteration

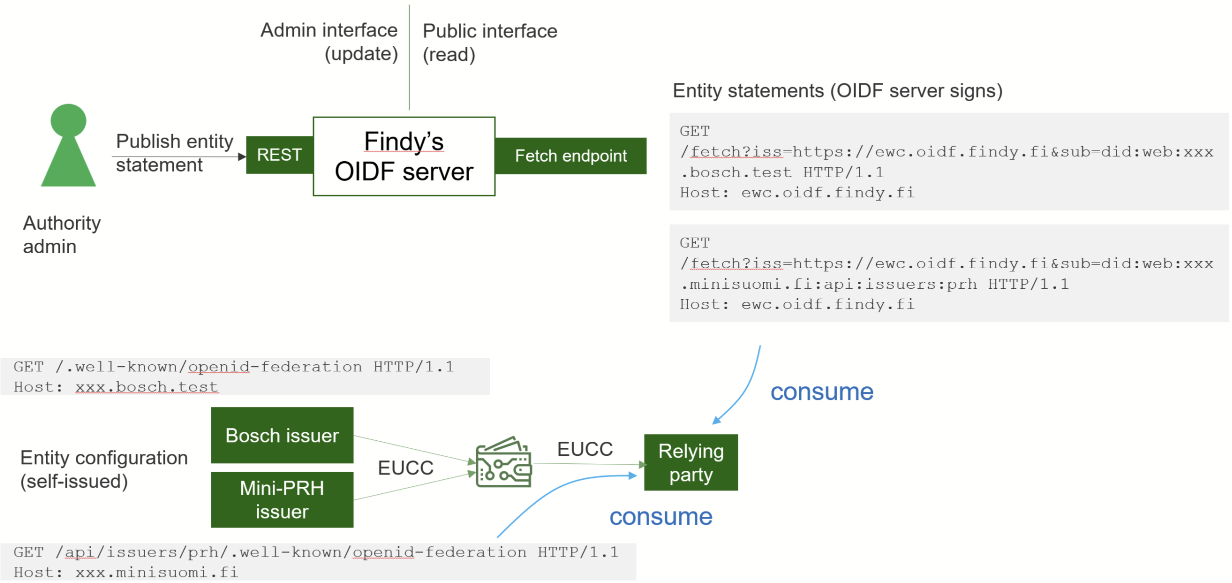
The third iteration was demonstrated in December 2024. In that iteration, KVK joined the pilot by issuing legal PID and EU company certificates to a Mini-Wallet from which they were

Co-funded by the European Union

presented to the relying party in the Finnish Tax Administration. Project internal recording on the demo of the 3rd iteration: https://nextcloud.ewc-consortium.eu/s/NLdkjTERgkoxpy3 . A full report on the 3rd iteration is available here.

In March and April 2025, real persons representing real companies were invited to join a user journey where they were provided test wallets with test identities and asked to walk through the flow of opening a bank account for a business in a test bank abroad. In the user testing, the test users completed the flow 72 times and carried out 336 transactions (issuing or presentation of an attestation). Summary of the user feedback is provided in chapter 4 (section 4.4) and a more detailed presentation here.

OpenID Federation service was used as a trust mechanism in iterations 2 and 3 and the user testing. The relying parties used OpenID Federation to ensure the attestations presented from the wallets were issued by an issuer registered to the OpenID Federation service. Figure 11 below illustrates the OpenID Federation infrastructure for the KYC pilot.



```
GET
/fetch?iss=https://ewc.oidf.findy.fi&sub=did:web:xxx
.bosch.test HTTP/1.1
Host: ewc.oidf.findy.fi
```

```
GET
/fetch?iss=https://ewc.oidf.findy.fi&sub=did:web:xxx
.minisuomi.fi:api:issuers:prh HTTP/1.1
Host: ewc.oidf.findy.fi
```

```
GET /.well-known/openid-federation HTTP/1.1
Host: xxx.bosch.test
```

```
GET /api/issuers/prh/.well-known/openid-federation HTTP/1.1
Host: xxx.minisuomi.fi
```

Figure 11 OpenID Federation infrastructure for KYC pilot

Findynet Co-operative hosted an OpenID Federation server instance which had:

- an admin interface through which an administrator could manage and publish entity statements in the server,
- a public interface through which anyone could fetch the published entity statements
- In the pilot setup, the administrator had published three subordinate entity statements in the OpenID Federation server,
- a subordinate entity statement describing the "Bosch issuer" that was the issuer of NPID, LPID and EUCC attestations for German users,
- a subordinate entity statement describing "Mini-DVV" that was the issuer for NPID attestations for Finnish natural persons (not present in the diagram above),
- a subordinate entity statement describing "Mini-PRH" that was the issuer for LPID and EUCC attestations for Finnish legal persons.

Furthermore, each entity had self-issued entity configuration statements available in its well-known endpoint.

Co-funded by
the European Union

The entity statements were fetched and evaluated by the relying party (i.e. online bank) in the pilot. Before accepting an attestation, the relying party made sure its issuer has a subordinate entity statement available in the OpenID Federation server.

3.5 P4.1.1 KYS 2.0 Peppol network registration and use (Transforming Supplier Verification in eInvoicing)

3.5.1 Pilot description

In the digital economy, businesses face growing challenges in verifying suppliers within eInvoicing networks like Peppol. Manual Know Your Supplier (KYS) processes are slow, repetitive, and prone to fraud—leading to financial risks, compliance burdens, and inefficiencies.

KYS 2.0 introduces a game-changing solution by combining Archipels Wallet, a trusted EUDI Wallet solution, with B2Brouter's leading eInvoicing platform (B2Brouter is the brand name of the beneficiary Invinet). The integration of both systems enables businesses to securely store, share, and verify supplier identity attributes – such as VAT numbers, legal names, and IBANs – ensuring seamless, secure and fraud-resistant supplier onboarding.

With KYS 2.0, companies benefit from:

- Automated supplier verification – Eliminate manual processes with instant, secure KYS checks.
- Stronger security and fraud prevention – Identity and IBAN verification reduce financial risks.
- Lower compliance costs – Digital identity management minimizes regulatory burdens.
- Frictionless eInvoicing integration – Verified credentials integrate directly into Peppol & other.

By leveraging Archipel's decentralized identity technology and Invinet's eInvoicing expertise, KYS 2.0 transforms supplier verification into a fast, secure, and fully automated process—empowering businesses to operate with confidence in the digital economy.

The challenge

European businesses face major hurdles in supplier verification, especially within eInvoicing networks like Peppol. Traditional KYS processes are:

- Time-consuming & repetitive
- Prone to errors & fraud (identity theft, IBAN fraud, fake invoices)
- Costly due to manual compliance efforts

With the rise of digital invoicing, businesses need a secure, efficient, and automated solution to onboard suppliers while ensuring authenticity and regulatory compliance.

The pilot scope

The pilot introduces a seamless, automated KYS solution that leverages the EUDI Wallet, allowing businesses to verify suppliers and securely exchange verified identity attributes (e.g., legal name, VAT number, IBAN) within eInvoicing networks.

The pilot proposes a streamlined, secure, and automated solution for the KYS processes specifically tailored for registering customers in eInvoicing networks like Peppol. The main improvements include:

- Automation of KYS processes: By automating parts of the KYS procedure, this solution reduces the manual workload and decreases the likelihood of human error. It simplifies repetitive verification tasks, leading to faster and more accurate customer onboarding.
- Enhanced security and fraud prevention: Implementing advanced verification methods, such as identity checks and IBAN authentication, reduces exposure to risks like identity theft, fraudulent invoices, and IBAN fraud. The system's security-focused design aims to safeguard businesses from potential financial losses and reputational damage.
- Cost reduction in compliance: Automated KYS procedures can be less resource-intensive, cutting down on compliance-related costs associated with labor, time, and regulatory adherence. This efficiency also makes KYS compliance more feasible for businesses of all sizes.

In the future it should be possible for businesses to automatically adapt identity attributes such as legal company name, legal address, VAT number during the creation of invoices or during the registration process for invoicing platforms and networks. This will ease the registration process and avoid manual and incorrect entries of master data. It will make the invoicing process more efficient, secure, and less resource-intensive, but also significantly faster. The automation of these processes will further reduce manual interventions, lowering costs, saving time, and minimizing errors. Additionally, stronger identity and IBAN verification processes directly address the vulnerabilities associated with identity theft and fraud. Businesses can be more confident in their transactions and relationships with verified suppliers, fostering trust across the eInvoicing network.

The **motivation and goals of the pilot** are the following:

The pilot demonstrates how to create a secure, efficient, and trustworthy eInvoicing ecosystem in which businesses across the EU can seamlessly onboard and interact within eInvoicing networks, like Peppol, with confidence in their counterparts' authenticity. By integrating automated KYS checks, the pilot aims to reduce the administrative burden, minimize fraud risks, and ensure regulatory compliance without significant costs or operational complexity. This future-ready approach prioritizes both security and ease of use, paving the way for a digital invoicing landscape where businesses can focus on growth and innovation, not regulatory hurdles or security threats.

EU businesses and citizens would experience a more secure, transparent, and efficient digital invoicing ecosystem, helping to build a stronger and more interconnected European economy:

Increased trust and security in business transactions: By ensuring the authenticity of suppliers and financial transactions, businesses gain confidence in their business relationships, making it safer to engage in new partnerships. This heightened trust reduces instances of fraud, which in turn supports overall economic stability and security.

Lower operational costs for businesses: Automated KYS procedures reduce the costs associated with manual verification and regulatory compliance, making it more affordable for small- and medium-sized businesses to participate in eInvoicing. This cost-saving potential is significant for EU businesses, freeing up resources for other operational needs.

Enhanced fraud prevention for EU consumers and businesses: The ideal implementation of this use case significantly reduces instances of identity theft, fake invoicing, and IBAN fraud, providing a more secure environment for all parties. This can lead to fewer financial losses and greater protection for businesses and consumers alike, fostering a safer digital financial ecosystem.

Economic and time efficiency: Automated KYS procedures would enable faster onboarding, allowing businesses to begin transacting digitally more quickly, thereby accelerating cash flow and reducing time spent on administrative tasks. This efficiency directly contributes to economic productivity and strengthens the business landscape across the EU.

Streamlined compliance with EU regulations: With integrated and automated KYS checks, businesses can stay compliant with regulatory standards without having to invest heavily in compliance infrastructure. This harmonizes with the EU's goals for streamlined, uniform digital invoicing, facilitating trade across borders within the single market.

3.5.2 State-of-the-art (SOTA) analysis

Currently, onboarding to eInvoicing networks like Peppol involves manual entry of company master data and submission of documentation as proof of registration (e.g., Peppol ID). On platforms like B2Brouter, which serves around 140,000 users, only a limited number are Peppol-enabled due to the complex and administrative-heavy activation process.

This registration workflow includes manual checks of scanned documents, requiring significant human effort to validate authenticity. Since there is no robust identity verification integrated into the process, it's not possible to reliably confirm the identity of the applicant, leaving systems vulnerable to fraud such as fake supplier identities or manipulated invoices. As a result, businesses may unintentionally engage in transactions with malicious actors.

Although Peppol and platforms like B2Brouter technically support digital invoicing, the lack of automated, secure KYS mechanisms hinder adoption and exposes networks to financial and compliance risks.

The central issue this use case tackles is the lack of trust, efficiency, and scalability in supplier onboarding for digital invoicing networks. Specifically, businesses face:

- High administrative burden from manual verification of identity documents.
- Increased risk of fraud, including fake invoicing, IBAN fraud, and identity theft.
- Barriers for small and medium enterprises to adopt digital invoicing due to compliance complexity and cost.

These challenges directly impact the ability of EU businesses to operate securely and efficiently within cross-border digital ecosystems. According to data from the B2Brouter platform, while over 140,000 businesses are users, only a fraction is Peppol-enabled, highlighting how current methods discourage full participation due to onboarding complexity and risk exposure.

The proposed solution introduces a secure, automated onboarding process for Peppol and similar eInvoicing networks through the integration of the EUDI Wallet. This approach allows:

- Automated transfer of verified identity attributes and master data (e.g., legal name, VAT ID, IBAN) when the user authenticates with their digital wallet.
- Streamlined verification of authenticity, with real-time checks against trusted sources.
- Immediate generation of a digitally signed service contract, allowing faster access to services like Peppol.

This future-oriented KYS process will:

- Boost trust and transaction security by ensuring only verified businesses can participate, reducing the risk of fraud.

- Cut operational costs, especially for SMEs, by replacing manual compliance tasks with automated checks.
- Speed up supplier onboarding, improving business agility and cash flow.
- Enhance regulatory compliance across the EU by embedding verification standards into the process.
- Support economic growth and innovation by allowing companies to focus on their core operations rather than complex administrative hurdles.

By prioritizing security, interoperability, and usability, this pilot solution lays the groundwork for a resilient and unified European digital invoicing environment, where businesses and consumers alike benefit from transparency, safety, and efficiency.

3.5.3 Business process overview and value

In the current process, the user must enter their master data manually and actively endeavour to use Peppol and provide corresponding proof that they have been assigned the respective identity attributes. On the B2Brouter side, this leads to effort and manual verification steps. For each user of the platform and Peppol, the validity and suitability of the proof submitted must be checked in order to verify a user. As it is currently not possible to check in this process whether the user is really who they claim to be, it is not possible to ensure that there is no fraud and that the corresponding proofs have not been falsified, particularly as current verification is based on scanned proofs and manual checks. In a threat scenario, fraudsters could, for example, send fake invoices to companies in the hope that they will be paid by the recipients.

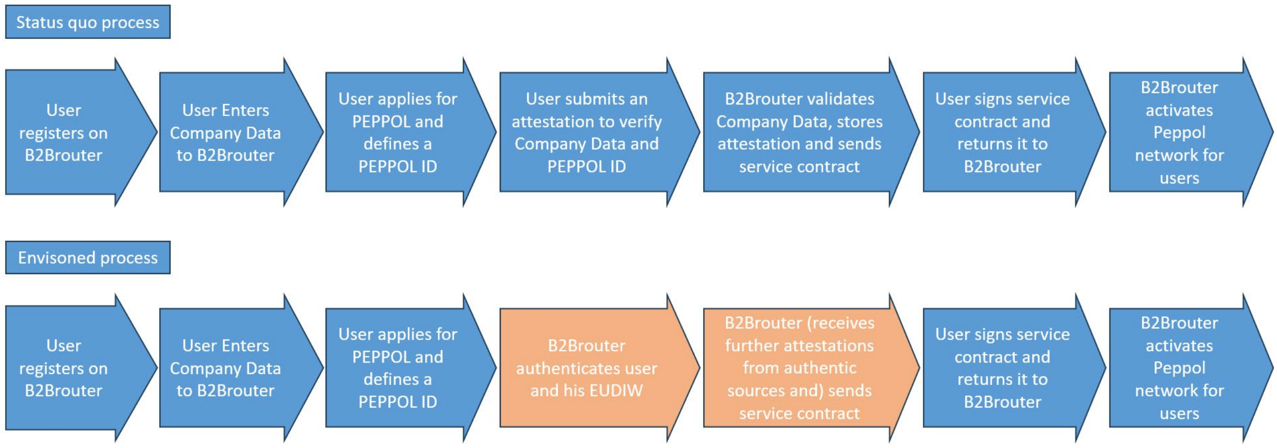

Status quo process
User registers on B2Brouter
User Enters Company Data to B2Brouter
User applies for PEPPOL and defines a PEPPOL ID
User submits an attestation to verify Company Data and PEPPOL ID
B2Brouter validates Company Data, stores attestation and sends service contract
User signs service contract and returns it to B2Brouter
B2Brouter activates Peppol network for users
Envisoned process
User registers on B2Brouter
User Enters Company Data to B2Brouter
User applies for PEPPOL and defines a PEPPOL ID
B2Brouter authenticates user and his EUDIW
B2Brouter (receives further attestations from authentic sources and) sends service contract
User signs service contract and returns it to B2Brouter
B2Brouter activates Peppol network for users

Figure 12 Verification process

The envisaged process (showed in Figure 12) assumes that authenticity proof, the provision of the company's data, as well as the verification of the identify attributes used for registration, can take place directly through the use of the EUDI Wallet. The user therefore authenticates himself with his wallet on the B2Brouter platform and the master data can be automatically transferred to the platform. At the same time, the identity attributes used for authentication are verified with corresponding evidence. After that, B2Brouter can provide an automated service contract with the corresponding identity attributes and master data for the customer to sign a service contract in order to use the Peppol network and potentially other platform services.

The implemented pilot solution in B2Brouter (Verifier) settles the following process to verify the data of the company/user (Holder) using the EUDI Wallet solution from Archipels (EUDI

Wallet Provider) and the QEAA issuer, InfoGreffe. The process is illustrated using screenshots of the implemented solution in Annex A: Company Verification process – B2BRouter Verifier.

Business Value

The pilot delivers substantial business value by demonstrating how a secure, interoperable, and user-friendly onboarding and verification process can transform eInvoicing across the EU. By automating KYS processes through the EUDI Wallet, the pilot eliminates key friction points in onboarding, enabling trustworthy digital transactions at scale. Businesses benefit from:

- Faster access to eInvoicing networks like Peppol
- Lower onboarding costs
- Improved fraud prevention
- Simplified regulatory compliance

These improvements enable organizations to accelerate time-to-value, reduce risks, and focus resources on growth rather than administrative overhead. For eInvoicing service providers like B2Brouter, the pilot also means reduced manual workload, scalable compliance, and an enhanced value proposition to their customer base.

3.5.4 Architecture and infrastructure

Figure 13 illustrates the high-level architecture used for implementing the scenario. B2Brouter in this scenario acts as verifier. B2Brouter implements an API provided by the Wallet solution provider Archipels that is able to verify the PID and (Q)EAA provided by issuers such as Infogreffe. The user then can present its data to the B2Brouter platform.

Similar to the EUDI Wallet provider, the (Q)EAA issuers and PID providers are registered in a list of trusted service providers. When the user enters the B2Brouter platform, it can use the EU-Wallet instance to authenticate and present its PID and eventual (Q)EAA that are needed to verify additional information such as VAT ID or IBAN to B2Brouter. By using the Verifier API of Archipels, B2Brouter can access the list of trusted Service Providers and can prove that the data presented is authentic.

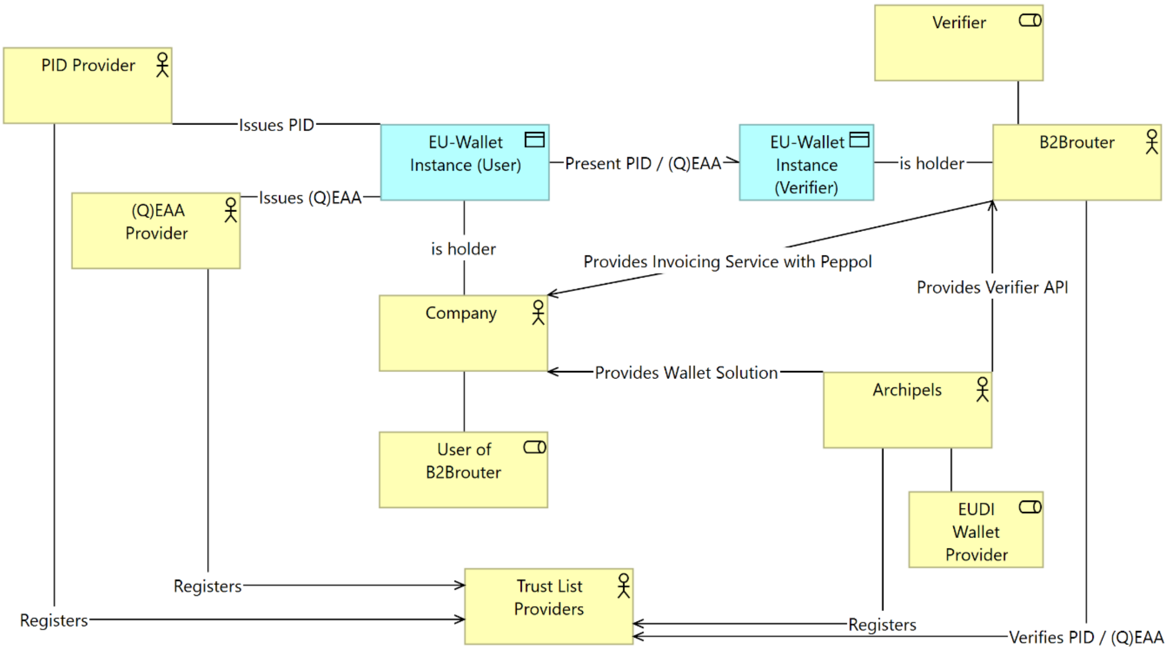


Figure 13 High-level architecture of verification

Figure 14 illustrates the key roles and processes that are associated with each scenario in EWC.

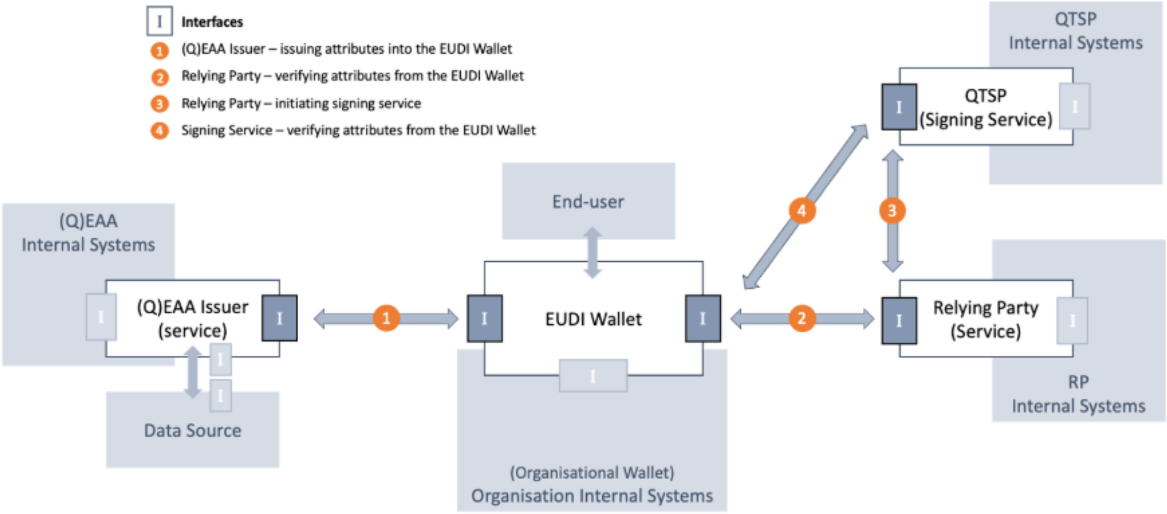
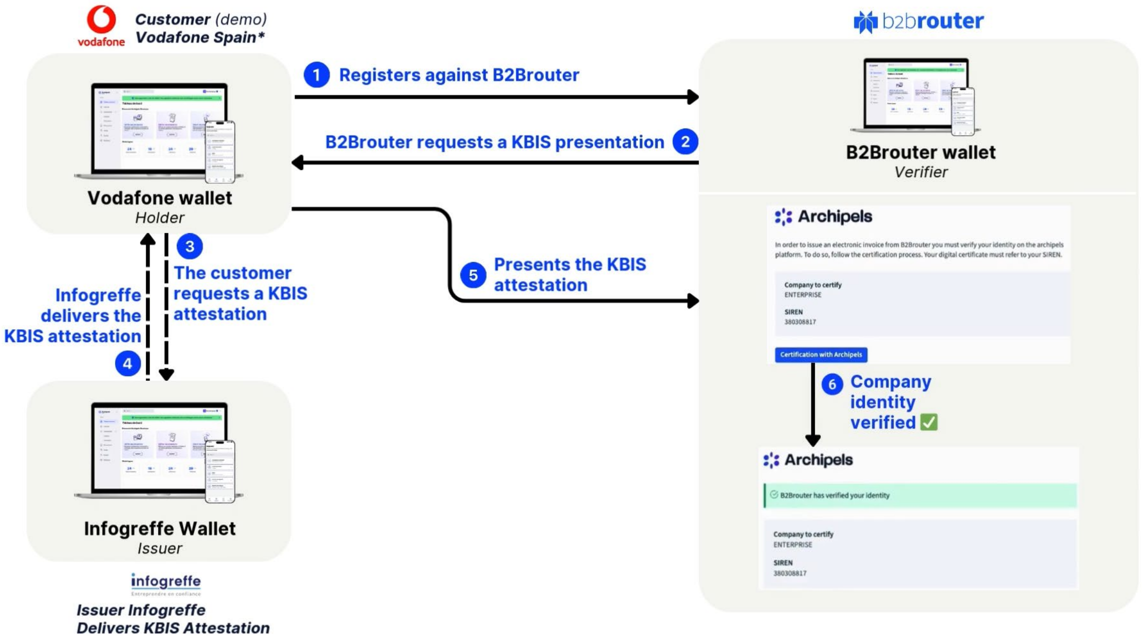

I Interfaces
1 (Q)EAA Issuer – issuing attributes into the EUDI Wallet
2 Relying Party – verifying attributes from the EUDI Wallet
3 Relying Party – initiating signing service
4 Signing Service – verifying attributes from the EUDI Wallet
QTSP Internal Systems
QTSP (Signing Service)
End-user
(Q)EAA Internal Systems
(Q)EAA Issuer (service)
EUDI Wallet
Relying Party (Service)
RP Internal Systems
Data Source
(Organisational Wallet) Organisation Internal Systems

Figure 14 Reference Architecture EWC

In the B2BRouter solution architecture the abstract reference architecture, shown in Figure 14 can be mapped upon the specific actors and processes that are implemented by the B2Brouter pilot. The pilot's specific solution architecture is illustrated in Figure 15.


vodafone
Customer (demo)
Vodafone Spain*
b2brouter
1 Registers against B2Brouter
B2Brouter requests a KBIS presentation 2
Vodafone wallet
Holder
B2Brouter wallet
Verifier
3 The customer requests a KBIS attestation
Infogreffe delivers the KBIS attestation 4
5 Presents the KBIS attestation
Archipels
Certification with Archipels
6 Company identity verified ✅
Archipels
Infogreffe Wallet
Issuer
infogreffe
Issuer Infogreffe
Delivers KBIS Attestation

In order to issue an electronic invoice from B2Brouter you must verify your identity on the archipels platform. To do so, follow the certification process. Your digital certificate must refer to your SIREN.

Company to certify
ENTERPRISE

SIREN
380308817

B2Brouter has verified your identity

Company to certify
ENTERPRISE

SIREN
380308817

Figure 15 Solution architecture of B2BRouter

In this solution architecture the end-user is the holder of an EUDI Wallet (e.g. Vodafone Spain).

1. It registers on B2Brouter, the Relying Party (Service) through the Web application.
2. The B2Brouter platform then asks the End-user to present its KBIS attestation to verify its account data.
3. Using Archipels EUDI Wallet solution as QTSP and its API, the end user can the request the KBIS attestation from the (Q)EEA Issuer (service) Infogreffe Wallet.
4. Infogreffe, being the (Q)EEA Issuer (service) delivers the KBIS attestation to the holder, Vodefone Spain, for approval using Archipels EUDI Wallet solution as QTSP
5. After approval, the user presents the KBIS attestation to B2Brouter, being the Relying Party (Service) by using the Archipels EUDI Wallet solution as QTSP.

A video of the demo presented at the Madrid GA is available at: https://www.youtube.com/watch?v=P36QEq57uh0

3.6 P4.2.1 Verifiable eReceipt

3.6.1 Pilot description

A Verifiable eReceipt (vReceipt) is a business document used by both natural and legal persons as a proof of purchase. The vReceipt can be used in a variety of business cases, such as accounting, financing, insurance, expense management, etc. The merchant issues the vReceipt to the natural person wallet of the buyer who, if necessary, presents the vReceipt to the verifier, such as their employer (for a cost/travel expense claim). Alternatively, the merchant may issue the vReceipt directly to the employer's wallet.

In the execution of this pilot, task 3.3 "Business Scenarios piloting" of WP3 joined forces with the WP2's travel/payment use case. In WP2 Phase 2 pilot, a person booking and paying a travel ticket from Fast Ferries could also optionally receive a vReceipt for the payment in their mobile wallet.

Furthermore, in phase 3 the issuance and storage of the vReceipt to the EUDI Wallet is automated as a direct result of a payment authorization (including identity verification) using the EUDI Wallet. The exact process is documented as part of EWC RFC-011 (Payments With Verifiable Receipts).

EWC partners involved:

- **Issuer of the vReceipts for the ferry tickets:** Fast Ferries/University of Aegean
- **Provider of wallets to buyers**: various EWC mobile wallet providers, such as iGrant.io, Lissi, ValidatedID
- **Relying party of vReceipts:** Finnish Tax Administration

The **motivation and goals** of the pilot are the following: The use of vReceipts has been increasing during the past years. The current market is fragmented and there is no interoperability or common protocols. This has led to a situation where vReceipt data is not usable widely by the buyers or other potential relying parties, who would need them (e.g. insurance agencies, accounting firms, employers, etc.). In addition, the current technical approach is dependent on card payment methods, and the discovery of the buyer requires complex integrations with card issuers and/or merchant systems and payment systems.

The main functional goal is to enable the flow of vReceipts from the seller to the natural or legal person's wallet, and subsequently to automated receipt processing in business use cases by the receivers. The complete technical flow for the issuance of the vReceipts is available at EWC RFC-011 (Payments with Verifiable Receipts).

3.6.1 State-of-the-art (SOTA) analysis

There is a long history for merchants issuing paper receipts for payments they receive. In the digital era, an electronic receipt (eReceipt) can also be sent to the buyer by e-mail in pdf format or issued to the merchant's closed customer loyalty platform where the customer can browse their past eReceipts. An eReceipt or a scanned copy of a paper receipt can also be presented to a third-party receiver, such as buyer's employer (for a travel expense/cost claim) or insurance company (for an insurance compensation).

In general, existing eReceipts do not contain structured machine-readable data or issuer's digital signature that enables their fully automated validation and processing by the receiver. This causes manual work in the receiver end and exposes the receiver to fraud, such as forged receipts. The recent development in AI has made commonly available tools that can easily generate photorealistic pictures of fake receipts.

In the context of the EUDI Wallet, delivering a vReceipt must be virtually effortless. Each additional user action – such as asking the citizen to scan several QR codes in sequence—injects friction, increases cognitive load, and sharply raises the risk that people abandon the flow before completion. Industry data show that "every extra step in a checkout flow creates an opportunity for drop-off," while HCI research highlights that multiple QR codes in the same interaction confuse users and often lead to failed or wrong scans; recent usability studies of identity-wallet prototypes echo these findings, flagging QR-code–related pain points as a key cause of frustration[12][13][14]

[12] https://arxiv.org/abs/1510.08210

[13] https://www.usenix.org/system/files/soups2022-korir.pdf

[14] https://bitly.com/blog/qr-codes-for-payment-software/

Verifiable eReceipt (vReceipt) is an electronic attestation of attributes that is digitally signed by the seller and issued to the buyer's (or their employer's) EUDI wallet. The structured (JSON) format of the receipt payload and its data model following the CEN/TS 16931-8 recommendation enables its automated processing in the receiver side. This increases the trust on the vReceipts and reduces receiver's manual work.

A key outcome was the design of an end-to-end flow that automatically issues a vReceipt immediately after a payment is authorized—and the payer's identity is verified using the EUDI Wallet for both authorization and identification—inside the EUDI Wallet with no user interaction required. The full specification is available in EWC RFC-011, "Payments with Verifiable Receipts".

This flow has passed feasibility testing and was piloted in EWC Phase 3, a cross-work-package initiative jointly led by WP2 and WP3 in production, i.e. authorizing real payment transactions paying for real tickets and issuing the resulting receipts to the EUDI Wallet.

3.6.2 Business process overview and value

The **current process** without the wallet is the following:

Merchant issues a paper or pdf receipt: Based on VAT and other relevant laws the merchant must issue a receipt as a proof of purchase to the purchaser. There is no common and structured model for the receipt, but laws may require certain data as a minimum content on the receipt. Technically, a receipt is in paper or in pdf. The merchant must record sales into his accounting and receipts or sales listing forms a basis for sales accounting. The data on sales is structured inside the accounting system of the merchant, but after the receipt is created it is shared and forwarded in pdf or in paper. There are some service providers who may transmit a receipt in a structured format. Nevertheless, most of the solutions are closed solutions where receipts are transmitted in pdf format.

Purchase for business purposes: Business clients purchase goods and services for economic activities, and have right to deduct them in accounting, direct and indirect (VAT) taxation. Business client needs a document to prove what was purchased and indicate for which deductible activity this purchase should be recorded. A receipt is one type of a document by which this might be proved. This is the reason why paper or pdf receipts must be attached to accounting vouchers. This procedure is either manual procedure, or a solution may help to recognise the most essential data on the receipt (scanners). When scanners are used, business clients must manage formats scanner recognises. A receipt may include other relevant data for internal accounting (inventory accounting or carbon footprint accounting), and these are normally out of scope of scanner-solutions.

Receipt operators: Some commercial chains have developed their own closed solutions where receipts may be stored normally as pictures. There are some operators which transmit receipts. These require that the merchant is able to make a receipt available and the merchant has to make an agreement with the operator. Main problem in these solutions are how the purchaser shares the address into which the merchant sends the receipt.

The following section describes the process **using the EUDIW** in relation to the pilot:

Rami (buyer) is an employee of a company and needs to do a business trip to a customer. Rami buys a ferry ticket from Fast Ferries. After the trip, Rami needs to claim the travel expenses from his employer. Two usage scenarios are supported.

In **Usage Scenario 1 (that contains two variants)**, Rami gets the vReceipt in his natural person wallet. This scenario has two operational variants, depending on how the vReceipt is triggered. The steps are shown in Table 3:

Table 3 Usage Scenario 1

Variant	**Flow**	**Key Difference**	**Pilot Phase**
1A – Point-of-sale initiated	1. Rami opens his EUDI Wallet, scans the QR code shown at the Fast Ferries checkout, and approves the merchant's request to issue a vReceipt. 2. The Fast Ferries point-of-sale (PoS) system packages the receipt data and Rami's eAddress, then relays both to the Fast Ferries issuer wallet. 3. The issuer wallet signs, issues, and transmits the vReceipt to Rami's wallet. 4. Rami later presents a cryptographic proof of the vReceipt to his employer. 5. The employer imports the vReceipt into its expense-management or accounting system.	Rami must interact with his wallet once at checkout (scan + approve).	2
1B – Payment-triggered, zero follow-up	1. Rami authorises the ticket payment in his EUDI Wallet and shares the identity attributes required by Fast Ferries. 2. The acquiring bank validates the payment and notifies Fast Ferries. 3. Fast Ferries' issuer wallet prepares the vReceipt; Rami's wallet polls and retrieves it automatically—no second interaction is needed. 4. Rami can later prove the vReceipt to his employer, which files it in its accounting system.	Rami interacts with the wallet only for payment; the vReceipt arrives automatically after bank confirmation.	3

In **Usage Scenario 2**, Rami does not have a wallet but asks the vReceipt to be issued directly to his employer's legal person wallet[15].

1. Rami indicates his employer's eAddress.
2. Fast Ferries' Point of Sale system hands the receipt contents and Rami's employer's eAddress to the issuer wallet of Fast Ferries.
3. Issuer wallet of Fast Ferries issues and sends the vReceipt to Rami's employer's wallet.
4. Rami's employer passes the vReceipt to its expense management/accounting system.

The **business values** vReceipts can provide are:

1. **Reduced manual work.** vReceipt is a machine-readable structured document. The receiver of the vReceipt is able to import its contents to the business systems automatically, with little or no manual steps. This reduces manual work and errors. The contents of the vReceipt can also be more detailed than those of the paper receipts.
2. **Preventing fraud.** The receiver of the vReceipt is able to validate that the vReceipt contents haven't been tampered with after it was issued.
3. **Identity and properties of vReceipt issuer.** The receiver of the vReceipt is able to learn who has issued the vReceipt (issuer's legal PID) and the issuer's properties (such as, legal form and status).

[15] This approach corresponds to an issuer-initiated flow which was not experimented in this pilot.

4. **Issuer's VAT status.** To be able to deduct the VAT that the vReceipt contains, the buyer can ensure the seller has a valid VAT number.
5. **Wallet address of the buyer/receiver**. The eAddress of the buyer's/receiver's wallet is presented to the Seller during the purchase transaction. Otherwise, the buyer must be able to remain anonymous.
6. **Post-sales channel to the buyer.** If supported by the technical protocols and unless opted out by the buyer, the transaction opens to the buyer's wallet a channel that can be used for post-sales purposes, such as, support, delivery of supplementary services and product withdrawals, if needed.
7. **Open interoperable ecosystem.** Unlike current closed digital receipt systems (often focused on a particular issuer or group of issuers), any seller could join the vReceipt ecosystem and start issuing interoperable vReceipts, provided they commit to the rules of the ecosystem.
8. **State-of-the-art user experience:** As of June 2025, no commercially available product unites payment authorization, selective disclosure of verified identity attributes, and the instant delivery of a cryptographically signed receipt inside the same identity wallet[16].

3.6.3 Architecture and infrastructure

The following system components were used:

- CFF (Fast ferries)/UAegean used their own issuer service for issuing vReceipts
  - For phase 3 a wallet connect service was implemented by UAegean that enables the merchant (Fast Ferries) to generate a payment request that triggers the issuance of a vReceipt at the end of the flow. Furthermore, for phase 3 Fast Ferries used iGrant.io as their organizational wallet.
- Mobile wallets used: common mobile wallets in EWC (Lissi, Validated ID, iGrant.io)
  - For phase 3, only the iGrant.io holder wallet will be used for piloting as this offer a payment native user experience and furthermore iGrant.io is collaborating directly with Banca Transilvania (BTRL) the bank accepting EUDI Wallet authorized payments in production. This ensures no interoperability issues will be observed.
- Relying Party: The Finnish Tax Administration used the Mini-Suomi/Mini-Wallet environment for the relying party functionality (https://vreceipt.minisuomi.fi/)
- vReceipt were issued using OID4VCI and presented using OID4VP standards. RFC-011 was prepared to describe how issuance of a vReceipt can be integrated to the EUDIW payment transaction.
- vReceipt used SD-JWT-VC structure
- vReceipt based on DS-011 schema: https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas/blob/main/data-schemas/ds011-vReceipts.json

Figure 16 and Figure 17 depict the usage scenarios 1 and 2 described in the Business Process Overview and Value section:

[16] https://support.apple.com/en-us/104954
https://support.google.com/wallet/answer/12060038?hl=en
https://www.fime.com/blog/blog-15/post/the-impact-of-digital-identity-on-payments-541
https://www.yoti.com/patents/

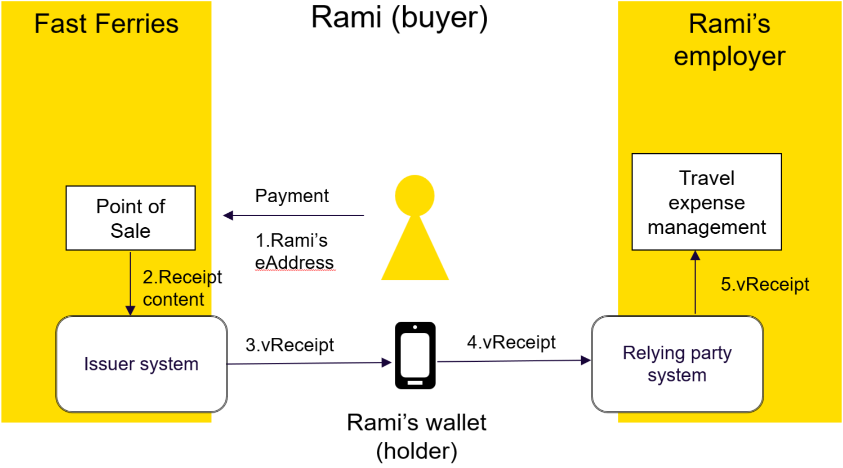


Figure 16 Usage scenario 1 - topology

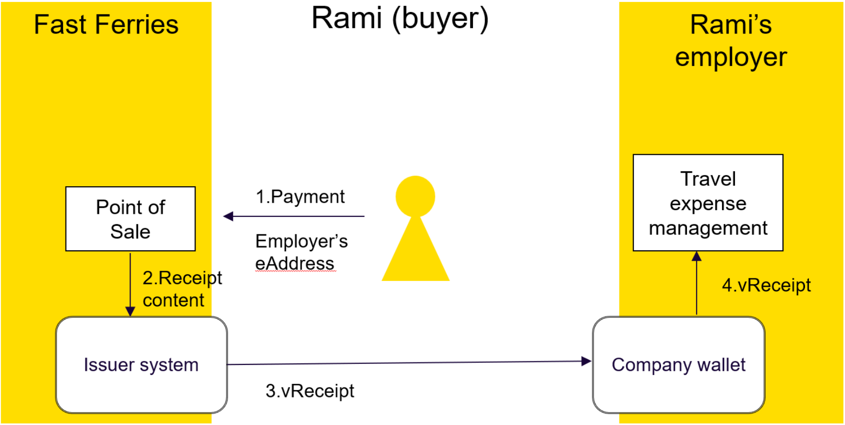


Figure 17 Usage scenario 2 - topology

Screenshots of the implementations of Fast Ferries and the Finnish Tax Administration, as well as the user journey are shown in ***Annex A: Fast Ferries / Vero – vReceipt interfaces***.

3.7 P4.3.1 Create a company branch in another country

3.7.1 Pilot description

This business scenario focuses on a company seeking to establish a branch in a country different from its registered office. Currently, this process is highly complex due to the reliance on manual controls, a lack of standardized procedures, limited security measures, and non-compliance with the proposed eIDAS 2.0 framework. The objectives of this scenario are threefold: 1) to enhance security and technical trust mechanisms for branch registration; 2) to explore the technical and legal challenges associated with compliance with eIDAS 2.0; and 3) to reduce lead times and minimize manual intervention in the registration process.

Brønnøysundregistrene, the Norwegian Business Registry, and Bolagsverket, the Swedish Business Registry, are collaborating to pilot this scenario under the initiative “Create a Branch in Another Country.” The main steps involve a Swedish company applying for branch registration with the Norwegian Business Registry, which, as part of this process, accepts the Swedish Certificate of Registration. The pilot may also explore the reverse process, where a Norwegian company registers a branch in Sweden.

Several stakeholders have a vested interest in this scenario. The primary stakeholders include wallet providers and businesses that utilize digital wallets and attestations from public authorities such as national business registries. Other public agencies also have an interest in this pilot, as it serves as a demonstration of the feasibility of cross-border digital business interactions. Additionally, financial institutions, including banks, may find value in the scenario as it could streamline business verification processes.

Disclaimer: The findings and processes described in this pilot are specific to the collaboration between the Swedish and Norwegian Business Registries. Technical discussions are based on existing systems and methodologies used in Sweden and Norway, and these processes may vary in other jurisdictions. However, these differences do not impede the execution of the pilot. It is also acknowledged that real-world implementation would involve additional legal and technical challenges that are not addressed within the scope of this pilot.

Table 4 shows the **EWC Partners involved**:

Table 4 Create company branch stakeholders involved

Actor	Roles	Actor within pilot
Business Registers • Bolagsverket (Sweden) acting as an Issuer • Brønnøysundsregistrene (Norway) acting as a Relying party	1. Authentic source 2. Relying Party 3. PUB-EAA provider 4. (Organizational) Wallet Holder	Yes
iGrant	Wallet provider	Yes
Test person and test company – Swedish test company with Norwegian representative	User – Natural person representative of a business with a natural person wallet acting as Holder and Relying Party Business – test organization for which a branch is created (not acting in any role)	N/A
Real business representatives for user tests	Real natural persons who previously have created branches in Norway with the mother company in Sweden	No agreement

The pilot focuses on key functionality necessary for enabling cross-border business attestation issuing and registration with the help of digital identity wallets. The main areas covered within the scope include:

- **PID issuance:** A Personal Identity (PID) credential is required for the natural person representative to authenticate with the business registry's e-services and initiate the branch registration process on behalf of the organization.
- **Schema definition for EUCC attestation**: A standardized schema for the EU Company Certificate (EUCC) attestation will be developed to ensure interoperability and consistent validation of company credentials.
- **EUCC issuance:** The issuance of an EUCC, along with potentially other company credentials, is necessary to provide the Norwegian Business Registry with trusted evidence regarding the parent company.
- **Functional wallet requirements for issuance:** The pilot will define the necessary functional requirements for wallets to support the issuance of credentials relevant to the business registration process.

- **User tests:** The evaluation of real representatives for companies who have previous experience in creating a company branch in order to understand if the process of creating a branch with a wallet seems understandable, easy and trustworthy.

Certain aspects are excluded from the pilot, primarily due to the absence of finalized technical specifications:

- **Security measures such as binding:** Mechanisms for binding credentials to holders or devices will not be implemented.
- **Wallet-based login:** Authentication using wallet attestations will not be supported.
- **Signing and sealing:** The signing or sealing of attestations and applications is not included in this phase.

Adaptation of internal business registry processes: The pilot does not involve changes to the internal workflows of business registries.

The **motivation and goals** of the pilot are the following: The pilot aims to establish a fully digitalized cross-border process for registration of a company branch. By leveraging digital identity wallets and trusted attestations, the initiative seeks to improve efficiency, security, and interoperability in business registration procedures.

3.7.2 State-of-the-art (SOTA) analysis

There are many steps before a branch can be started at Bolagsverket or Brønnøysundregisterne. These are similar processes, here we are describing the process at Bolagsverket.

- First, the parent company needs to send a registration form for the branch to Bolagsverket. This is done by paper nowadays.
- Second, the CEO needs to be registered, including the CEO's power of attorney in original and attested. The power of attorney needs to contain information that the parent company gives the CEO power to act in all decisions of the branch, can accept summons for the branch, can speak and answer for the branch alone. The Power of attorney needs to be dated and signed by signatories according to the correct rules. Bolagsverket provides templates for such power of attorneys.
- Furthermore, a proof of registration of the parent company, letters of association, annual accounts of the two previous years, and a certificate of non-bankruptcy (not older than 6 months and issued by the business registry of the parent company country) needs to be sent to Bolagsverket.
- Thirdly, all branches that conduct financial operations need to register an official auditor.
- When all information and payment have arrived at Bolagsverket, the branch name needs to be controlled. It is not a given that the branch can have the same name as the parent company.
- Finally, when Bolagsverket decides on registering the branch it will get an organization number and a proof of registration.

All proofs are being sent by post, they are paper documents and need to manually be approved. There is no digital process for this at the moment. The case officers are entering all information manually in the systems and scan documents. For all branch matters, official notices for additional information have to be sent out, since something is always missed, which increases the lead times.

Statistic: Bolagsverket has 5 FTE working on branch matters.

During the period analysed, an average of approximately 257 branch registration cases were received per month. The number of formal requests for clarification or additional documentation (“förelägganden”) was nearly equal, averaging 256 per month. This suggests that nearly every case results in at least one such request. The number of actual completions or responses to these requests (“kompletteringar”) was slightly lower, averaging 240 per month. This indicates that some cases may involve multiple follow-ups, while others may be resolved without the need for additional input.

The average processing time per case was approximately 69 days. This relatively long lead time is likely influenced by the high number of requests for additional information. It is reasonable to assume that the more completions a case requires, the longer it will take to process.

Overall, the statistics suggest that the handling of branch registration cases is relatively complex and involves frequent interaction between the authority and the applicant. There appears to be a clear correlation between the number of formal requests, completions, and the total processing time.

Based on the statistics of types of formal request types (“förelägganden”) for branch case matters issued between 2019 and 2025 in branch registration cases, clear patterns emerge in terms of which types are most commonly and consistently used.

The three most prominent types, measured by their average presence per year, are:

1. Submit information about the foreign company (Code 400)
2. Submit a description of the foreign company’s activities (Code 403)
3. Submit evidence showing that the foreign company is registered (Code 404)

These requests appear consistently in every year of the dataset, indicating that they are fundamental to the branch registration process in Sweden. Their persistent use suggests that they represent essential documentation needed to establish the identity, legal status, and intended business of the foreign company.

The high frequency of these requests also implies that applicants may often omit this documentation in the initial submission and that these items are part of a standard verification process applied to nearly all cases.

From a regulatory and process improvement perspective, this pattern highlights an opportunity to streamline case handling by improving how these core requirements are communicated to applicants.

Submitting these types of information in a streamlined process via attestations and the wallet might help in reducing the caseload in asking for this basic information and it might reduce the lead times for finishing the application for registering a branch.

The use case aims at (at least partly) digitalizing an entire manual process. The challenges that are solved with this are the long lead times, manual errors, administrative burden, lowering costs for businesses and the business registry, the lack of trustworthy and verifiable documents, and the lack of standardization of information.

The “Create Company Branch” use case introduces the ability to present structured, verifiable company credentials digitally via the EUDI Wallet, enabling (semi-) automated registering, pre-filling and controls in the business registry eService, and cross-border validation when registering a branch. The digitalization of the create company branch process is expected to lead to reduced lead times, time/cost savings, reduced legal risks, easier access and transparency into the process for businesses and a better user experience.

3.7.3 Business process overview and value

The process overview is the following:

Pre-conditions:

1. A Swedish company wants to start a branch in Norway.
2. The Swedish company has an EUID, equivalent to a Norwegian limited liability company such as AS, ASA, or SE.
3. The Swedish company has no address in Norway.
4. The company registers for the first time in the Register of Business Enterprises.
5. The Swedish company has a general manager which is also the applicant. The applicant has a Norwegian national identification number, is liable for an NPID and has a digital wallet.
6. The applicant is the general manager/submitter/fee payer and contact person, as well as the sole board member/chairperson of the company. Therefore, he or she has the signatory rights for the company.

Steps for the pilot:

Applicants:

1. Search and find the landing page of the Create Norwegian Company branch
2. Read information about Create branch services and what is needed
3. Navigate to the Norwegian Issuer of NPID and claims and download an NPID attestation
4. Navigate to the Swedish company registration office and claims and download an EUCC attestation
5. Start creating Company branch registration form service by establishing a connection to a wallet by scanning a QR code.
6. Receive presentation requests in the wallet and provide necessary attestations to establish a new branch (NPID, EUCC)
7. Fill in missing data in “create branch” registration form
8. Sign and submit registration of branch with sharing NPID attestation
9. Receive presentation requests in the wallet
10. Claims receipt attestation to their wallet.
11. Receive presentation requests in the wallet

Figure 18 depicts the flow for creating a branch at Brønnøysundregistrene.

Co-funded by
the European Union

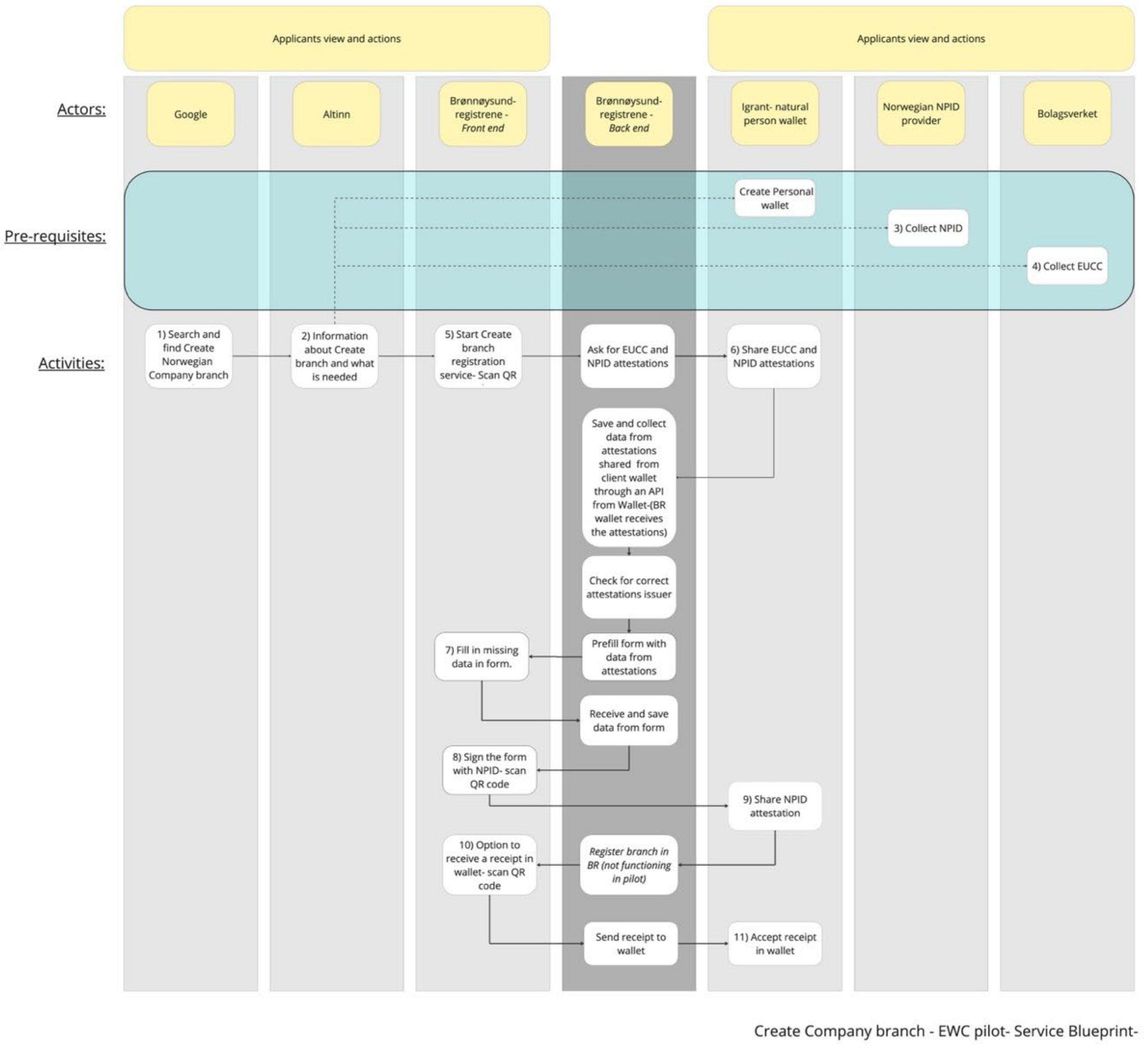

Applicants view and actions
Applicants view and actions
Actors:
Google
Altinn
Brønnøysund-registrene - Front end
Brønnøysund-registrene - Back end
Igrant- natural person wallet
Norwegian NPID provider
Bolagsverket
Pre-requisites:
Create Personal wallet
3) Collect NPID
4) Collect EUCC
Activities:
1) Search and find Create Norwegian Company branch
2) Information about Create branch and what is needed
5) Start Create branch registration service- Scan QR
Ask for EUCC and NPID attestations
6) Share EUCC and NPID attestations
Save and collect data from attestations shared from client wallet through an API from Wallet-(BR wallet receives the attestations)
Check for correct attestations issuer
7) Fill in missing data in form.
Prefill form with data from attestations
Receive and save data from form
8) Sign the form with NPID- scan QR code
9) Share NPID attestation
10) Option to receive a receipt in wallet- scan QR code
Register branch in BR (not functioning in pilot)
Send receipt to wallet
11) Accept receipt in wallet
Create Company branch - EWC pilot- Service Blueprint-

Figure 18 Create company branch - Service Blueprint

The **business value** of the pilot is depicted by Figure 19.

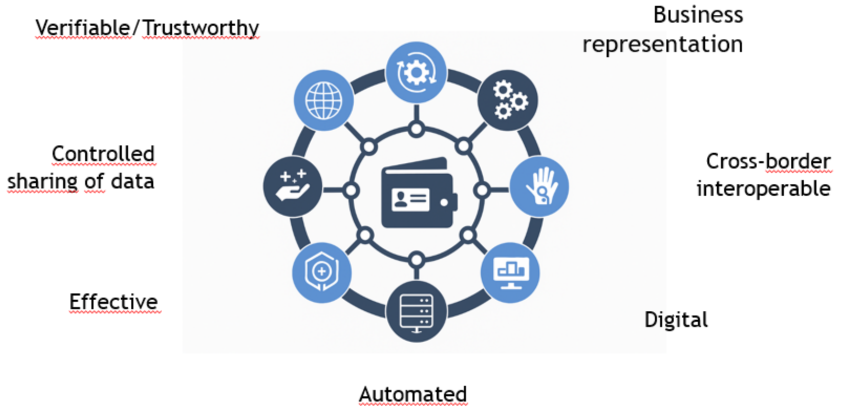


Figure 19 Business value overview of the create company branch pilot

More specifically:

1. **Automation of Verification and Validation:** Currently, attestations and documents submitted as part of branch registration cannot be reliably verified. Manual checks are prone to error, and there is no guarantee that documents are genuine. With digital

identity wallets, these controls can be (semi-)automated. Attestations—such as signatory rights or proof of company existence—can be issued by trusted sources and presented in verifiable formats. Qualified electronic signatures can be automatically checked against trusted lists, ensuring authenticity in a traceable and consistent manner.

2. **End-to-End Digital Process with Fewer Errors:** By eliminating manual steps, the risk of human error in verifying or interpreting data is significantly reduced. Wallets enable structured, machine-readable data that can be directly processed by business registries and tax authorities—avoiding data entry mistakes and rework.
3. **Dramatic Reduction in Lead Time and Administrative Effort:** Today, it can take up to three months to collect and process all the information required to establish a company branch. At Bolagsverket, five full-time employees are dedicated solely to managing branch-related tasks. Wallets can reduce or eliminate delays caused by mailing documents, correcting incomplete submissions, or clarifying requirements. Stakeholders can receive validated data instantly and act on it without intermediaries.
4. **Controlled and Minimal Data Sharing:** The current process often results in applicants over-sharing sensitive information—such as full annual accounts—due to unclear requirements and fear of rejection. With wallets, applicants can present only the specific attestations required, improving privacy and efficiency. Verifiable credentials support selective disclosure, meaning only relevant data is shared.
5. **Seamless Cross-Border Interoperability:** Thanks to common semantic data definitions and European standards under the eIDAS 2.0 framework, digital wallets support cross-border use. Attestations issued in one EU country can be automatically recognized and understood in another. This understanding makes it easier for businesses to establish themselves across the EU.
6. **Reliable Business Representation:** Business representation – such as proving signatory rights, ultimate beneficial ownership (UBO), or a Power of Attorney (EU PoA) – is currently based on paper documents that are difficult or impossible to verify. In a wallet-based model, these are cryptographically signed, verifiable credentials, enabling secure and transparent delegation of authority.
7. **Stronger Protection Against Fraud and Data Breaches:** The importance of trustworthy digital interactions is underscored by findings from ENISA's Threat Landscape Report 2022[17]. The report notes a 68% increase in data compromises over 2020 and highlights that compromised credentials were the most common cause of data breaches, with an average cost of USD 4.24 million in 2021, according to IBM. These breaches affect not only financial integrity but also the reputation of businesses. A verifiable identity framework helps mitigate these risks by reducing reliance on static, easily compromised credentials.

3.7.4 Architecture and Infrastructure

Figure 20 shows an overview diagram of architecture and topology.

[17] European Union Agency for Cybersecurity (ENISA). ENISA Thread Landscape 2022 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

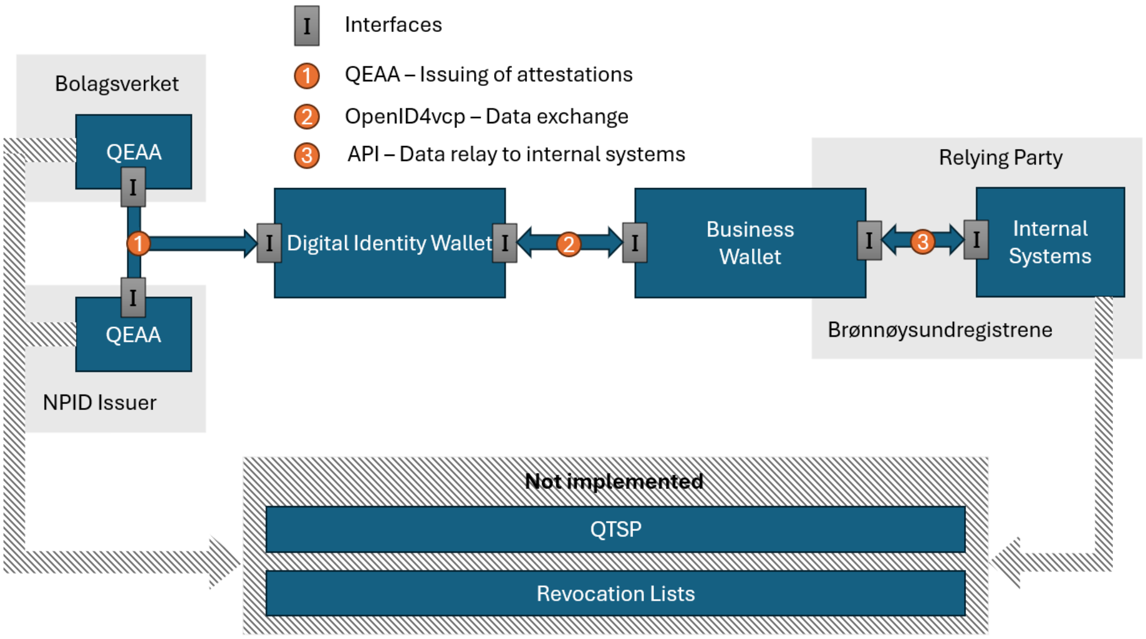


Figure 20 Infrastructure diagram

This pilot leverages the iGrant organisational wallet for issuing EUCC and the iGrant natural person wallet for presenting organisational attestations. Attestations are issued in the SD-JWT format, with issuance handled via the OpenID4VCI protocol and presentation conducted using the OpenID4VP protocol.

This pilot utilizes the LPID and EUCC attestations, which have been established in collaboration with other business registries and are publicly available at: eudi-wallet-rulebooks-and-schemas on GitHub.

In Figure 20, for the issuing process, Bolagsverket is the (Q)EAA (or rather PUB-EAA). Test data are fetched from the registers. Since there are no standardized interfaces defined yet towards authentic sources, iGrant's custom APIs are used (1 in Figure 20) to provide Bolagsverket's organizational wallet (EUDI wallet in Figure 20) with values for the generation of attestations. For issuing attestations to a natural person wallet, the OpenID4VCI protocol is used (1 in Figure 20).

The relying party (Brønnøysundregistrene) uses OpenID4VCP to accept presentations from the iGrant natural person wallet.

3.8 P4.4.1 Company Authorized Business Travel and eInvoicing

3.8.1 Pilot description

Employee (E) of Company (C) wants to travel for business. His trip expenses will be covered by the company. The company issues a custom PoA attestation, authorizing the employee to make expenses on behalf of the company for the purposes of the trip.

The booking of the ticket(s) will be made using the site of a Travel Agency (A). The travel agency site will require the employee to identify their identity (NPID) using a OID4VP flow, as well as the identity of the Company (LPID/EUCC).

After verifying both the Employee's and Company's identities, a custom PoA attestation is presented, proving that the employee is authorized to travel.

Finally, the employee books the trip tickets, and an electronic Invoice is sent directly to the Company through the Peppol Network.

EWC partners involved:

- Stellar travel agency acting as a Relying Party
- Telesto/Invinet (Netsmart technologies) acting as technological partners
- B2BRouter (commercial name of Invinet) as a Peppol Service Provider that sends the invoice on behalf of the travel agency
- Finnish Tax Authority (Vero) provided Mini-DVV as test issuer and Mini-Wallet as test company wallet
- Brønnøysundregistrene, the Norwegian Business Registry issuing LPID and EUCC attestations.
- iGrant acting as wallet provider

The pilot focuses on demonstrating verifiable credentials (VC) based flow where an employee books a business trip using authorization issued by their company. The employee is not a legal representative and acts on authorization granted by the company.

Certain aspects are considered as out of scope:

- LoA high requirements and trust framework
- Integration with real-world identity providers or production-ready Peppol Service Providers

The **pilot's motivation and goals** are the following:

- Authorizing employees to perform business-related actions, such as booking business trips, typically involves cumbersome, manual and email-based processes that lack standardization and verifiability. This leads to inefficiencies for both employees and the companies.
- The use of Verifiable Credentials and standardized OID4VP flows present a promising solution to automate those interactions. The pilot aims to explore the integration of EUDIW flows can be applied in a business travel scenario.

Goals:

- Demonstrate digital authorization and delegation
- Enable seamless booking experience
- Reduce cost and time
- Automate post-transaction invoicing (ensure eInvoice is sent directly to Company)

3.8.2 State-of-the-art (SOTA) analysis

Currently business trip bookings and expense management today often involve manual and fragmented processes for both identity verification and authorization. Travel agencies typically rely on user-typed information and unauthenticated email exchanges, without any reliable mechanism to confirm whether the person booking is an actual employee with authority to make expenses. Even when internal approvals and processes are set in place, they often take the form of lengthy email trails that are difficult to audit and prone to errors or miscommunication. Employees frequently pay with corporate or personal cards and then later submit expense claims. According to a recent study, **83% of business travelers** struggle to reconcile trip expenses, while **24% lack the time to submit claims** (TravelPerk, 2025)**[18]**.

Alternatively, billing by direct invoicing, requires the travel agency to manually verify billing details often through unstructured PDF documents or email exchanges which creates friction, administrative burden increases the risk of misbilling.

By introducing the use of the EUDIW and verifiable attestations, the pilot addresses the following challenges:

- **Lack of verified identity and role:** The Travel Agency cannot confidently verify that the person booking is an authorized employee.
- **Missing proof of authorization:** Current processes do not allow travel agents to confirm if the employee has permissions to do expenses.
- **Manual and error-prone invoicing:** Invoice routing manually relies on free-text input and unverified data, increasing the risk of misbilling.
- **Limit overspending:** There is no guarantee that the employee won't overspend and exceed budget limitations for the business trip.

The pilot introduces EUDIW and verifiable attestation sharing to replace the manual and unreliable processes with verifiable, machine-readable data. All attestations are presented securely via the wallet and get validated in real time by the travel agency service.

In addition, Peppol eInvoicing is used to automate invoice delivery directly to the company, using verified data from the LPID credential to look up and send to the correct Peppol participant of the Company.

In combining verifiable attestations and automated eInvoicing, the pilot lays the groundwork for more efficient business travel procedures across the EU, reducing administrative overhead.

3.8.3 Business process overview and value

Generally, the main actors and roles involved in the business trip process are the following:

- **Company (C):** Uses a valid server-based company wallet instance and grants authorization (PoA) to the employee to travel and do expenses on its behalf
- **Employee (E):** Natural person who acts as the holder of the PoA attestation and books the business trip
- **Travel Agency (A):** Acts as the Relying Party and verifies the presented attestations
- **Certified Peppol Service Provider:** Handles the submission of the eInvoice directly to the company via the Peppol network.

The following section outlines the typical steps that an employee currently follows to book a business trip:

1. **Trip search:** Employee visits travel agency site and selects travel and hotel options.
2. **Identity declaration:** Employee fills in personal and company details manually. There is no verifiable proof of authorization or link to the company.
3. **Authorization:** Employee provides proof of authorization, frequently an email from manager or internal approval request. Email exchanges are informal, non-verifiable and non-auditable.

[18] TravelPerk Press Release, 2025 - https://www.travelperk.com/press-release/latest-research-83-of-employees-struggle-with-travel-expenses-with-1-in-4-business-travelers-taking-the-financial-strain-themselves

4. **Invoicing:** Employee enters company billing info manually or uses corporate card. Invoice routing is done manually and there is a high risk of error.
5. **Expense management:** Employee must pay and submit expense claims later which requires internal validation and processing.

The following section outlines the process enabled by the EUDI Wallet ecosystem:

1. **Trip search:** Employee visits travel agency site and selects travel and hotel options.
2. **Identity declaration:** Employee is prompted to present attestations via EUDI Wallet (e.g., NPID, LPID, EUCC and PoA).
3. **Verification:** Travel Agency system automatically verifies the attestations in real-time (including financial budget requirements and authorization through PoA).
4. **Automated Invoicing:** Using details found on LPID, the Travel Agency automatically looks up the company's Peppol participant ID and sends invoice directly.

The **business value** of this pilot is to demonstrate how the integration of the EUDI Wallet can bring trust, automation and accountability into everyday B2B transactions. It enables employees to digitally prove both their identity and their authority to act on behalf of their company using verifiable attestations. This eliminates the need for manual checks, informal email trails and unstructured documentation improving and securing the booking process. The pilot also delivers tangible value by streamlining invoicing. Through the use of structured company data from the wallet, the Travel Agency can automatically bill the Company without relying on the employee to handle or forward billing details. This use case would reduce administrative effort, lower operational costs and enhance trust and efficiency in everyday business workflows

3.8.4 Architecture and infrastructure

The pilot was conducted in two iterations.

1st iteration

The first iteration ran during Phase 2 of EWC and was completed in May 2025. It was demonstrated in EWC General Assembly held in Stockholm in May. Figure 21 illustrates the architecture used in this iteration. In that iteration, attestations (LPID, EUCC and NPID) were issued by the Mini-DVV test issuer of the Finnish Tax Administration (Vero) and Power of Attorney (PoA) issued by a self-issued test issuer provided by the Mini-Suomi environment. The company wallet used was the Mini-Wallet, while the personal wallet used was iGrant's mobile data wallet app. Stellar travels, which is a Greek travel agency, acted as the Relying Party. No QSTP was used and was out of scope.

A video of the demo presented at the Stockholm GA is available at: https://nextcloud.ewc-consortium.eu/s/qwqKc7oQ2BdsqpA

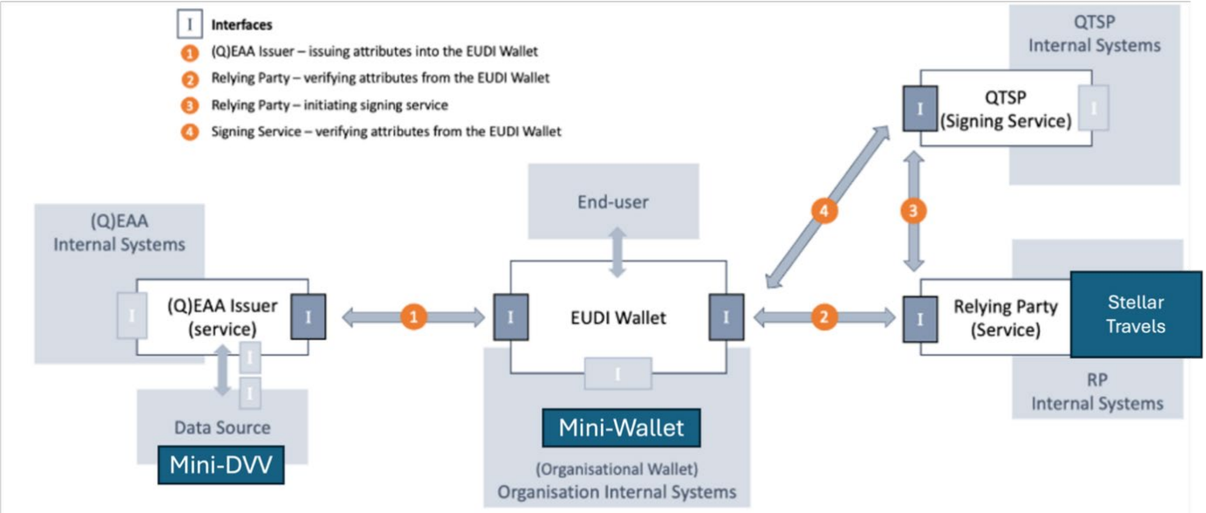

I Interfaces
1 (Q)EAA Issuer – issuing attributes into the EUDI Wallet
2 Relying Party – verifying attributes from the EUDI Wallet
3 Relying Party – initiating signing service
4 Signing Service – verifying attributes from the EUDI Wallet
QTSP Internal Systems
QTSP (Signing Service)
End-user
(Q)EAA Internal Systems
(Q)EAA Issuer (service)
EUDI Wallet
Relying Party (Service)
Stellar Travels
RP Internal Systems
Data Source
Mini-DVV
Mini-Wallet
(Organisational Wallet) Organisation Internal Systems

Figure 21 Overview diagram of 1st iteration of company authorized travel pilot

2nd iteration

The second iteration, shown in Figure 22, was completed in July 2025. In this iteration, Brønnøysundregistrene and DFO joined by issuing the LPID, EUCC and NPID attestations. The PoA attestation was issued using iGrant's Issuer API. The company wallet used was iGrant's Dev Enterprise wallet, and the personal wallet used was iGrant's data wallet mobile app. Stellar travels acted again as the Relying Party.

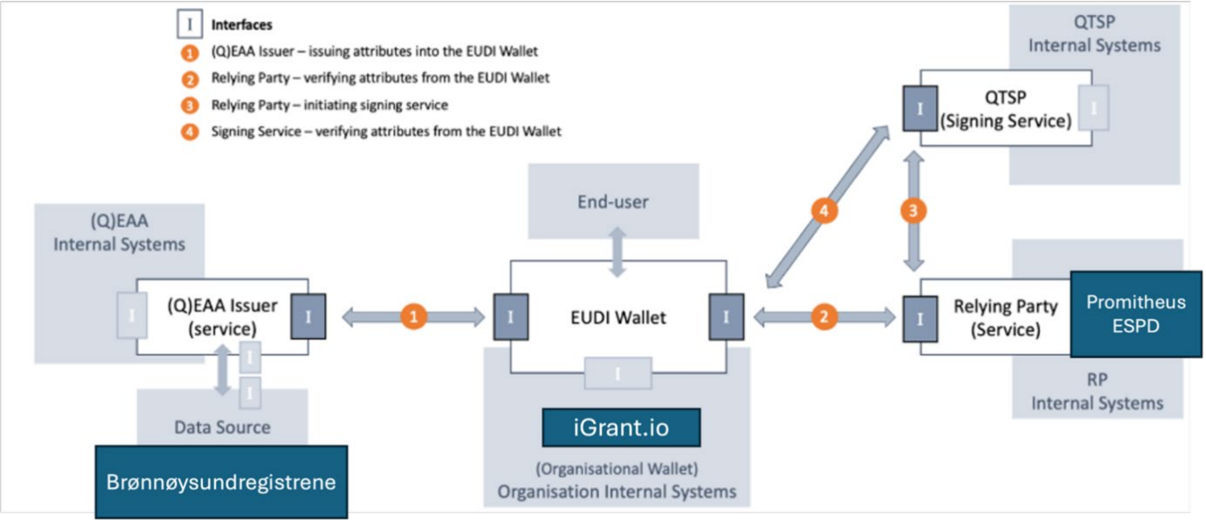

I Interfaces
1 (Q)EAA Issuer – issuing attributes into the EUDI Wallet
2 Relying Party – verifying attributes from the EUDI Wallet
3 Relying Party – initiating signing service
4 Signing Service – verifying attributes from the EUDI Wallet
QTSP Internal Systems
QTSP (Signing Service)
End-user
(Q)EAA Internal Systems
(Q)EAA Issuer (service)
EUDI Wallet
Relying Party (Service)
Promitheus ESPD
RP Internal Systems
Data Source
Brønnøysundregistrene
iGrant.io
(Organisational Wallet) Organisation Internal Systems

Figure 22 Overview diagram of 2nd iteration of company authorized travel

The following section describes the pilot in greater detail. The issuing of attestations is out-of-scope. The pilot begins by assuming that all attestations are already received in the respective wallets and focuses on presenting them.

Pre-requisites:

- Company has issued PoA attestation to Employee's wallet. Employee's wallet has also been issued a valid NPID.
- Company wallet has been issued valid EUCC and LPID attestations.

The pilot steps include:

1. **Authentication with individual digital wallet:** The Employee logins into the Travel agency site by scanning a QR code that represents a OID4VP NPID presentation request created by the Travel Agency site (Verifier)
2. **Verification of identity:** The Travel Agency verifies the identity of the Employee
3. **Employee provides eAddress or openIdOrganisationId[19]**: Following successful login, the employee provides the company's wallet eAddress or openIdOrganisationId to the Travel Agency by filling a form field.
4. **Travel Agency requests for LPID and EUCC presentation**: Using the eAddress or openIdOrganisationId received earlier, the Travel Agency makes LPID and EUCC presentation requests to the company's wallet.
5. **Company data presentation**: The company wallet responds with the LPID and EUCC data
6. **Travel Agency verifies LPID and EUCC data**: Travel Agency cross-checks and verifies LPID and EUCC data.
7. **Travel Agency requests for PoA**: Employee scans QR code representing the OID4VP based PoA presentation request created by the Travel Agency
8. **Employee proceeds on booking the trip**: The Employee proceeds on booking the trip. The Travel Agency verifies that the selected trip parameters are within the budget limits and dates found in the PoA
9. **eInvoicing**: The Travel Agency sends a Peppol based eInvoice to the Company through the Peppol Network.

Figure 23 shows a sequence diagram visualizing the above-described steps of the Company Authorized Business Travel and eInvoicing pilot.

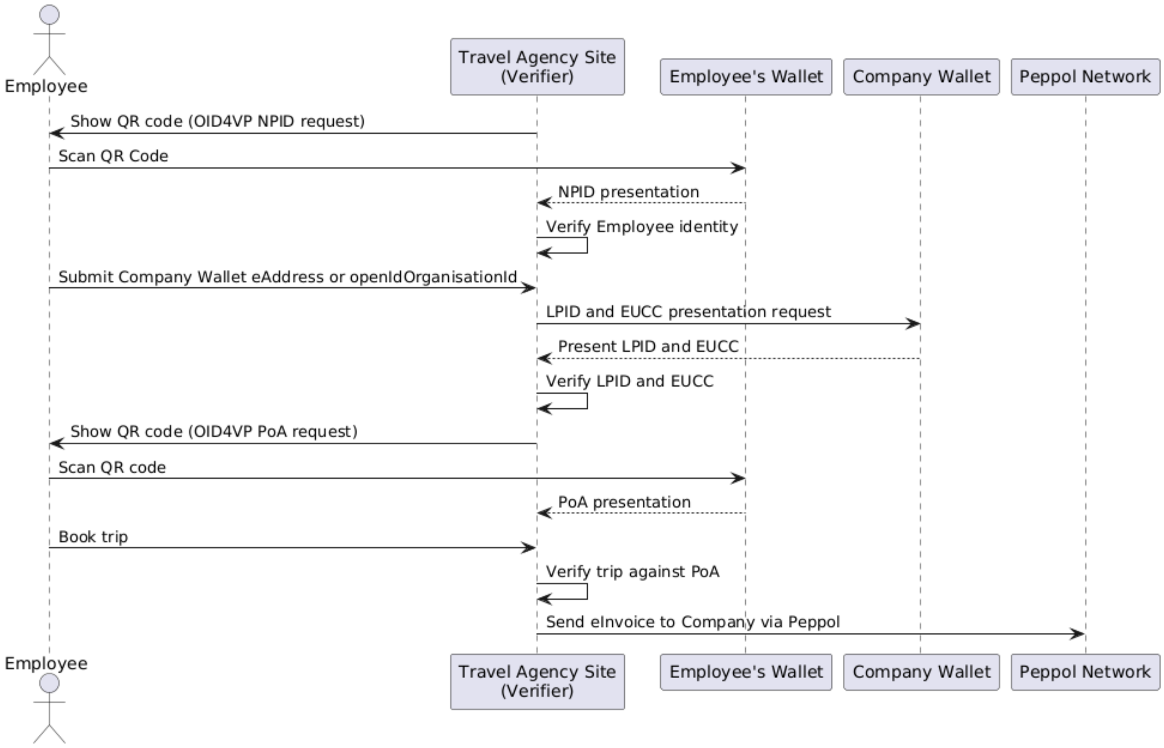


Figure 23 Company authorized business travel and eInvoicing sequence diagram

[19] The first iteration of the pilot supported eAddress as the mechanism for invoking the company wallet. However, since eAddress is not standardized, it was replaced with openIdOrganizationId in the second iteration.

4. EWC Pilots Evaluation

The following chapter provides a structure evaluation of the pilots implemented in EWC. Each pilot is evaluated using the following common structure:

- Assessment Summary, which includes the
  - achievement of own defined goals
  - level of ambition achieved
- Execution context (e.g., production, test)
- User testing feedback
- Insights and lessons learned, and
- Recommendations for the future

4.1 P1.1.1 Issue and verify attestations for evidence in the procurement process (ESPD)

4.1.1 Assessment summary

The following tables provide an overall assessment of the pilot. The first table evaluates the pilot's performance against its own defined goals, while the second assesses the extent to which the pilot achieved its intended ambition level.

Table 5 P1.1.1 own goals evaluation table

Goal Description	Rate (1-5)*	Comments
A public authority can issue certificates that are verifiable, authentic and always up to date	Not Applicable	After we started working on the pilot, it became clear that this goal was outside the scope, and it was redefined as a prerequisite to be able to go through with the pilot. DFØ is not in a position to issue LPIDs or certificates, this has to be done by Brønnøysundregistrene and other public authorities such as the National Tax Administration.
A legal entity can collect, use and share certificates using the EUDIW.	5	The pilot demonstrated with success that legal entities could collect, use and share a test-LPID via a tender platform using the EUDIW.
That public contractors can use EUDIW to trust that their contracts are performed as agreed.	Not Available	Due to revocation lists not yet being implemented we were unable to test the sharing of always-up-to-date credentials. However, we know this will be possible to test soon, and should be a goal for a future pilot.

***(Rates from 1 = not achieved to 5= fully achieved or N/A = Not Applicable, Not Available)**

Table 6 P.1.1.1 evaluation on ambition level achievement

KPI	Target planned within pilot	Achieved	Please specify names of the achieved KPIs	Comment: if your commitment differs from

				the initially planned (D3.5), explain why
Number of wallet issuing countries	1	1	Norway	
Number of ODI issuing countries	1	1	Norway; Brønnøysundregistrene	
QEAA (PubEAAs)	2	1 (below original target)	LPID issued from Brønnøysundregistrene.	Skatteetaten (Tax Admin) were not ready to issue VC's in time for the pilot due to internal issues.
Number of relying parties	1	4 (above original target)	Oslo municipality (CA, relaying party), Innkjøpskontoret (CA, relaying party), Artifik (tender platform, relaying party), Kantega (temporary evidence service, "relaying relying" party)	
QTSP providers	1	1	Same as "Number of wallets issuing countries"	
Wallet users (legal persons)	10	~20 (above original target)	Innkjøpskontoret (1 person), Crayon (3 persons), Dustin (2 persons) and Telia (3 persons), all acting as Economic Operators/holders. In addition, several others observing the pilot from both DFØ and Brreg joined in and tested the procedure.	
Wallet users (natural persons)	N/A	~20 (above original target)	Same as above, all users log in as a natural person to access the legal person wallet	
Number of transactions completed	N/A	~40 (above original target)	All participants collected an LPID from Brønnøysundregistrene and shared this with Kantega/Artifik.	

Co-funded by
the European Union

Number of qualified signatures issued	10	N/A	-	This pilot did not use wallet for signing; it was never part of the scope. The target said 10 qualified signatures, but this must have been a typo in the D3.5.
Number of ODI credentials shared	10	~20 (above original target)	All participants shared their test-LPIDs in the pilot	

4.1.2 Pilot execution in production environment

Table 7 P1.1.1 execution context

Name of the system	Production	Pre-production /acceptance	Clone of production built for the pilot	New prototype built for the pilot
Kantega evidence studio				X
Artifik tender platform			X	

The evidence studio was built purely for this pilot and will not be a standard feature. It was created to lessen the workload of Artifik and the need for modifications to their tender platform. Artifik created a connection with the evidence studio to collect attestations in their test environment.

Artifik will have to develop similar functionality as the evidence studio from Kantega in the future to be able to collect attestations.

The pilot performed more than 40 transactions, first collecting LPIDs from Brønnøysundregistrene and then sharing the LPIDs via Kantega and Artifik. See table of KPIs above for more information.

4.1.3 Pilot user testing feedback

There were plenum interviews/discussions done with the participants after conducting the pilots. Open questions were used as follows:

- What is your initial reflection around the pilot you have just participated in?
- As an EO, what are your thoughts on how this will affect your work regarding participating in public procurement when this technology becomes available?
- As a CA, what are your thoughts on how this will affect your work regarding administering procurement processes within this technology becomes available?
- As a CA, what are your reflections regarding trusting the documentation from the wallet?
- What do you miss from this pilot, or what would you like to pilot next time?

The EOs were instantly very positive to the pilot, as they could see the benefit of collecting the credentials once to the wallet and then sharing these in various tender processes. This will reduce manual work and the administrative burden of replying to public procurement processes.

The CA already had a high level of trust in the documentation they receive today, but they could see the benefit of receiving credentials directly from the source and not in a PDF that can be altered. We discussed a potential cross-border procurement with less known foreign documentation, and how that would affect their level of trust. Based on the replies from this user group we have an assumption that there is a high level of trust in Norwegian documentation simply because it is Norwegian (both in PDF and via wallet), and that the users did not fully understand that it is the wallet technology that provides the trust in the credentials. Meaning that they still perceived documentation via wallet from other countries just as “difficult” to trust as a foreign PDF is today. This is something that needs to be looked into further and to be communicated clearly in future pilots and potential launch of actual wallet services.

The potential this technology offers in terms of data minimization was also discussed. That means that instead of presenting the entire credential with all data, the CAs are just presented a proof of documentation, meaning the issuer confirms that the data is valid without the need of the CA controlling the actual data. This was too early to test in this pilot, but the CA saw this as a major potential for reduction of manual work and administrative burden.

The users expressed great interest in participating in future pilots with more complexity, different types of credentials and real data. The EOs were also very eager to test delegation functionality within the wallet. If the person with signatory rights, e.g., CEO, can delegate the collection and sharing of credentials to a bid manager, this will dramatically reduce the administrative burden for EOs. The participants accepted that this was an early pilot to test the basic data flow, but for them it is more interesting to test new user functionality to see more specifically how this technology can improve their work and efficiency.

The tender platform system was very interest in participating in further pilots to improve their functionality and prepare for new technology. DFØ have also been contacted by other actors in Norway delivering tender platform services that have expressed great interest in joining future pilots after hearing about this pilot.

4.1.4 Insight and lessons learnt

Our first plan for the pilot was to shadow an actual procurement, but this proved to be very difficult due to timing of the procurement, marked dialogue etc. In addition, Brønnøysundregistrene (BR) were not ready to pilot real data, so we landed on a compromise to use test data with real users. This way we could interview the EOs and CAs after the pilot and gain more insight into their actual needs.

The feedback on the pilot from the EOs was very positive, the wallet would be an instant time saver for them when engaging in public procurement processes. The CA was also positive; they also saw a potential time saver in receiving validated credentials that they could trust. One issue we discovered during the interviews after the pilot was that the participants did not quite grasp why the technology behind the wallet created higher security than the pdf’s they are used to. There is a very high level of trust in the Norwegian society, and the fact that DFØ and BR conducted this pilot was probably the reason for the trust. When communicating to the Norwegian public about wallet, it will be important to emphasize how the technology creates the security, and that it is the same across borders and credentials from other countries.

The intention was to include verified credentials from both BR and the Tax Authorities (Skatt) in this pilot, but only BR were ready to issue LPIDs and VCs within the time frame. Skatt have not formally been a part of the EWC until the very end of the project, but they have been actively included in the procurement pilot planning since December 2024. They are close to finalizing how they will produce a tax certificate as a verifiable credential, this would be great to test in a future pilot.

An important feature / possibility with using wallet technology for public procurement is the continued sharing and revocation of VCs. This is not yet ready for testing, but this will be an important part of further piloting with public procurement.

The procurement pilot involves many different stakeholders such as issuers, one wallet provider, one CA, several EOs, enterprise software) contribute to complexity for the pilot. Planning, meetings and communication take a lot of time and delays the process. This needs to be taken into account for planning the timeline for future pilots, particularly if it involves an actual procurement process.

The collaboration between DFØ, BR and Skatt in particular, but also across the Nordic countries, throughout the EWC piloting has been very good and an important success factor. The teams have different strengths and competencies, and we have shared knowledge, experiences and expertise.

4.1.5 Recommendations

- Contracting authorities need to understand the security benefits of the use of the business wallet and attestations especially for cross-border transactions and evidences satisfying inclusion and exclusion criteria from economic operators of other countries.
- More pilots need to be done to test the use of business wallets in different scenarios in public procurement, especially continued sharing and revocation of attestations, to demonstrate the benefits of using business wallets in the whole public procurement cycle.

4.2 P1.1.2 Automated verification of Economic Operator identity in the procurement process flow (ESPD)

4.2.1 Assessment summary

The following tables provide an overall assessment of the pilot. The first table evaluates the pilot's performance against its own defined goals, while the second assesses the extent to which the pilot achieved its intended ambition level.

Table 8 P1.1.2 own goals evaluation table

Goal Description	Rate (1-5)*	Comments
Simplify the use of an ESPD service by companies	4	The pilot demonstrated successfully how the EUDI wallet can be integrated into the ESPD process and automatically populate the ESPD form with validated data, reducing manual steps and repetitive data entry for Economic Operators.
Lower administrative burden on companies	4	Verifiable attestations (NPID, LPID, EUCC) reduce the need for scanning and uploading unstructured PDF documents.

Goal Description	Rate (1-5)*	Comments
Prevent fraud by verifying company identity	3	The use of digitally signed attestations issued from trusted sources ensure the authenticity and the integrity of the presented identity, potentially helping fraud prevention. However, the underlying trust infrastructure (such as trust anchors) was not fully implemented.

***(Rates from 1 = not achieved to 5= fully achieved or N/A = Not Applicable, Not Available)**

Table 9 P.1.1.2 evaluation on ambition level achievement

KPI	Target planned within pilot	Achieved	Please specify names of the achieved KPIs	Comment: if your commitment differs from the initially planned (D3.5), explain why
Number of wallet issuing countries	2	2	Norway, Finland	
Number of ODI issuing countries	2	2	Norway, Finland	
QEAA (PubEAAs)	2	3	LPID, NPID, EUCC	
Number of relying parties	1	1	Greek ESPD Service (Promitheus)	
QTSP providers	1	0	Trust framework was not implemented	Trust anchors and infrastructure were not implemented
Wallet users (legal persons)	10	2	1 Finnish Company, 1 Norwegian Company In addition, several others observing the pilot from both UPRC, Telesto, and Netsmart joined in and tested the procedure.	From a technical perspective, integration with Sweden would also been possible, as the Norwegian credential issuer operates under the same infrastructure used by the Swedish Business Register. However, due to time constraints within EWC, the Swedish cross-border scenario could not be tested.

Co-funded by the European Union

Wallet users (natural persons)	N/A	2	1 Finnish Legal representative, 1 Norwegian Legal Representative	
Number of transactions completed	N/A	6	Finnish EUCC, NPID, LPID. Norwegian EUCC, NPID, LPID	
Number of qualified signatures issued	10	-	-	
Number of ODI credentials shared	10	2	EUCC, LPID	D3.5 reports 3 as target planned. It is a typo, should be 2.

4.2.2 Pilot execution in production environment

The pilot run in a **pre-production** environment of the Promitheus ESPD Service which is based on ESPD EDM (Exchange Data Model) v3.3.0. As part of the pilot, a new prototype Verifier component was developed. This component acts as a wrapper for OID4VP based presentation and verification functionalities, designed for easy integration with the existing ESPD system architecture. It is built with re-usability in mind allowing the same component to be deployed across multiple pilots (such as the “Company authorized business travel and eInvoicing” pilot) and can be extended in future projects involving verifiable attestations.

Table 10 P1.1.2 execution context

Name of the system	Production	Pre-production /acceptance	Clone of production built for the pilot	New prototype built for the pilot
Promitheus (ESPD Service)		X		
Verifier				X

The transactions performed were the presentation of EUCC and LPIDs for Norwegian and Finnish companies, along with NPIDs of their respective Legal Representatives. All data used in the pilot were test data and did not represent real companies of natural persons.

4.2.3 Pilot user testing feedback

Due to limited time and focusing more on the cross-border interoperability dimension (implementation of two iterations) and conformance testing with the EWC test best, no formal user testing with structured user testing questionnaire was conducted. Testing was limited to engaging test users that were aware of the process of ESPD filling in and submission, being themselves legal representatives of their respective companies and having created ESPD responses to specific ESPD requests in order to participate in Greek tenders.

The test users went through the whole process in both iterations and commented that:

- The wallet enables ecosystem significantly reduced time that is usually spent on manual entry and cross-checking information compared to traditional ESPD creation process.
- It can potentially reduce the administrative burden and help businesses seek and participate in cross-border business opportunities.
- There was inconsistency in how credentials are presented in the 1st iteration. Company attestations are presented via eAddress, while the NPID was shared using a QR code. This mixed approach made the process feel fragmented.

4.2.4 Insights and lessons learnt

Interoperability issues

Interoperability issues arise between wallet implementations, Issuers, and Relying Parties. For example, some wallets may only support a specific client_id_scheme, requiring Relying Party to accommodate multiple-schemes and all the different OID4VP presentation request fields for each scheme. Additionally, there is no guarantee of backwards compatibility. If a wallet implementation upgrades to OID4VP draft 19, while the Relying Party still uses OID4VP draft 18 the interaction may break due to incompatibilities between versions.

Lack of technical readiness and technical examples

Many issuers are not yet technically prepared to issue verifiable attestations (VCs). The technical flows can be complex, especially for those without prior experience with OID4VC. Providing a test EWC reference issuer and verifier would help developers better understand and experiment with the complete OID4VCI and OID4VP flows, facilitating learning and adoption.

Security concerns

There is no high LoA available, and the trust framework is not implemented yet. Security concerns will arise when it comes to real-world transactions.

Lack of standardization of wallet invocation mechanisms

There is no standardization for wallet invocation mechanisms, which introduced integration complexity between implementation phases. During the initial phase of the pilot, the Finnish wallet (Mini-Wallet) supported invocation using eAddress based requests. However, in the later phase involving the Norwegian use case, the Enterprise wallet solution (iGrant) did not support invocation through eAddress presentation requests. This required further changes and added technical overhead.

It is recommended to align on standardizing invocation protocols/mechanisms. A consistent approach will enhance interoperability across wallet providers and Relying Parties, especially in cross-border scenarios.

4.2.5 Recommendations

- Have stable and mature specifications, as interop testing gets very challenging with different versions of specifications.
- Provide a test reference issuer and verifier which would help developers to better understand and experiment with the complete OID4VCI and OID4VP flows, facilitating learning and adoption.
- Implement a trust framework that can be used in order to scale to deployment and production transactions.

- Work on the standardisation of wallet invocation mechanisms.

4.3 P2.1.1 Onboarding new business partner

Archipels exited the EWC project before the ending of the project. Therefore, they did not complete the pilot evaluation against its own goals and targeted KPIs. They only provided an interim assessment with the achieved KPIs at that moment, and some lessons learnt and future recommendations that are presented in the respective sections below.

4.3.1 Assessment summary

The following table presents the pilot achieved KPIs versus its intended ambition level at the point of interim assessment on M22.

Table 11 P.2.1.1 evaluation on ambition level achievement

KPI	Target planned within pilot	Achieved	Please specify names of the achieved KPIs	Comment: if your commitment differs from the initially planned (D3.5), explain why
Number of wallet issuing countries	1	1	France	
Number of ODI issuing countries	2	1	France	The pilot with the Netherlands was not completed.
QEAA (PubEAAs)	3 to 4	5	LPID, EUCC, IBAN, Signatory rights, UBO	
Number of relying parties	7+	7		Recruited by Infogreffe
QTSP providers	3	2		At this stage no attestation provider is qualified.
Wallet users (legal persons)	30+	14		
Wallet users (natural persons)	30+	17		
Number of transactions completed	TBC	TBC		
Number of qualified signatures issued	TBC	0		Not piloted
Number of ODI credentials shared	100+	Not available		

4.3.2 Insights and lessons learnt

The main issue encountered during the piloting phase was the lack of engagement from the companies enrolled in the KYS pilot. From the discussion we had with our testers we identified some explanations:

Adoption:

- The beginning of our piloting (Q1 2024) was too early stage. On one side our wallet wasn’t fully ready to onboard suppliers, so we began the test in several phases and lost interest from the testers before we could deliver the complete test workflow. The other reason seems to be that the companies still have no idea of what the EUDIW is

Co-funded by
the European Union

and eIDAS 2.0 and the generalization of the wallet will be a game changer for them. The lack of emergency for them to be ready to integrate the wallet in their process did not help to keep them prioritizing their participation to the pilot.

- Companies want to use solutions that can answer a need or a problem fully. For the KYS business scenario we proposed a partial workflow with only some of the document exchanged during the onboarding of a business partner (EUCC and IBAN) to comply with limited data availability. Testers mentioned that they would be more interested in the wallet if it had all the documents needed to do a supplier onboarding.
- The adoption of the legal person wallet is strongly linked to its ecosystem adoption of the wallet. Organizations need to be able to interact with their business partners.
- The concept of wallet, attestations, authentic source, verification, trusted source, trust registry are still new and complicated to assimilate for companies with no digital experience.

UX quality:

From the interviews we did with the future users of the wallet (operational employees) and the legal representatives (who only help to verify the wallet), we had very clear feedback that every UX errors or misunderstandings were an obstacle to the wallet adoption.

We worked a lot with our UX and UI team to improve the design and messaging of our wallet to reach positive feedback about it. Users felt reassured once the wallet was clear and had a clean design.

Communication:

One of our conclusions is that the Legal person EUDIW must be a subject of pedagogic communication from the EU and Member States so the future users can understand the goal behind its use.

4.3.3 Recommendations

- Develop adoption strategies for disseminating the value and benefits of business wallets and convince companies using business wallets for doing business simply and digitally.
- Do more work on UX/UI in order to facilitate wallet adoption.
- Develop plans for educating businesses and making them believe that the business wallet is trustworthy and is great for making business simply and digitally.

4.4 P2.2.1 Open a bank account for a business

4.4.1 Assessment summary

The following tables provide an overall assessment of the pilot. The first table evaluates the pilot’s performance against its own defined goals, while the second assesses the extent to which the pilot achieved its intended ambition level.

Table 12 P2.2.1 own goals evaluation table

Goal Description	Rate (1-5) *	Comments
Using an EUDIW for organizations to open bank account cross-border remotely.	4	We demonstrated how the flow could work, including legal person representative's authentication and power of attorney. Some attestations (in particular, ultimate beneficial owner certificate) were not implemented, but once available their integration to the flow is similar.
Reduce fraud and cut costs for financial institution's regulated KYC processes.	4	The actual KYC checks were not part of the pilot but based on the bank feedback we managed to demonstrate the value for the banks' processes.

Table 13 P2.2.1 evaluation on ambition level achievement

KPI	Target planned within pilot	Achieved	Please specify names of the achieved KPIs	Comment: if your commitment differs from the initially planned (D3.5), explain why
Number of wallet issuing countries	3	LP: 2 NP:2	Legal person wallets: Finland (Vero), Germany (Bosch) Natural person/mobile wallets: Sweden (iGrant.io), Germany (Lissi)	
Number of ODI issuing countries		3	Finland (Vero), Germany (Bosch), the Netherlands (KVK)	No target set
QEAA (PubEAAs)	0	0	No QEAA audits possible during the project timeframe	
Number of relying parties	3	3	Vero relying party (1st and 3rd iteration) Bosch relying party (2nd iteration) Fictive Bank AG relying party, provided by Bosch (user testing)	

QTSP providers	0	0	No QTSP providers in the pilot	
Wallet users (legal persons)	15	72	The number of end users who completed the flow of opening a business account in the user testing in March-April 2025	
Wallet users (natural persons)	0	86	The number of end users who requested and received a natural person identification data (NPID) in their mobile wallet as part of the user testing in March-April 2025	Initially natural person wallets were not planned to be used
Number of transactions completed	45	336	Total number of attestations (NPID, LPID, EUCC) issued and presented in the user testing in March-April 2025	
Number of qualified signatures issued	0	0	No QES signatures in the pilot	
Number of ODI credentials shared	2	3	Legal PID, EU Company Certificate and Power of Attorney	

4.4.2 Pilot execution in production environment

Steps toward production environment

The test environment mini-Finland was used for testing. Mini-Finland is an open platform for co-development in development projects. On the platform, parties are able to model solutions and test data-transfers between parties. Solutions created and tested on the platform are not directly production ready solutions. Below we have described next steps towards the production.

Integrated App-service should replace virtual environment used for test purposes. App-service should include services for issuers, holders and verifiers. The structure could be subnet-solution. A key vault for private keys should be created to store them securely. The database should be based on PostgreSQL instead of SQLlite. PostgreSQL is normally used for enterprise solutions and covers functionalities needed in enterprise solutions and is more scalable.

The Issuer API should have identification and authorisation functionalities instead of open log-in for test purposes. The issuer API should also have user log functionalities to monitor users. GDPR and data security statements should be created. A data security testing should be done. The code should be finalised. The double CSRF pattern should be created to mitigate CSRF attacks. The functionality to save attributes more secure should be designed. A trust network for wallets should be created to replace a federated service offered by Findy co-operative.

Table 14 P2.2.1 execution context

Name of the system	Production	Pre-production /acceptance	Clone of production built for the pilot	New prototype built for the pilot
Issuer (NPID, LPID, EUCC)				X
Wallet				X
Relying Party (bank)				X

The total number of transactions were 336, which is translated to the total number of attestations (NPID, LPID, EUCC) issued and presented in the user testing in March-April 2025.

4.4.3 Pilot user testing feedback

In March 2025, the pilot environment was exposed for user testing to Finnish company representatives with background in financial management of companies. No previous experience on wallets was expected. In the user testing, 26 users followed instructions to walk through the user journey where they used natural and legal person wallets with test identities to open an account in a test bank. This section shortly highlights the results. Full user testing feedback is available here. The questionnaire is available in ***Annex B: Open a bank account – Digital Wallet Trial User Feedback form.***

Co-funded by the European Union

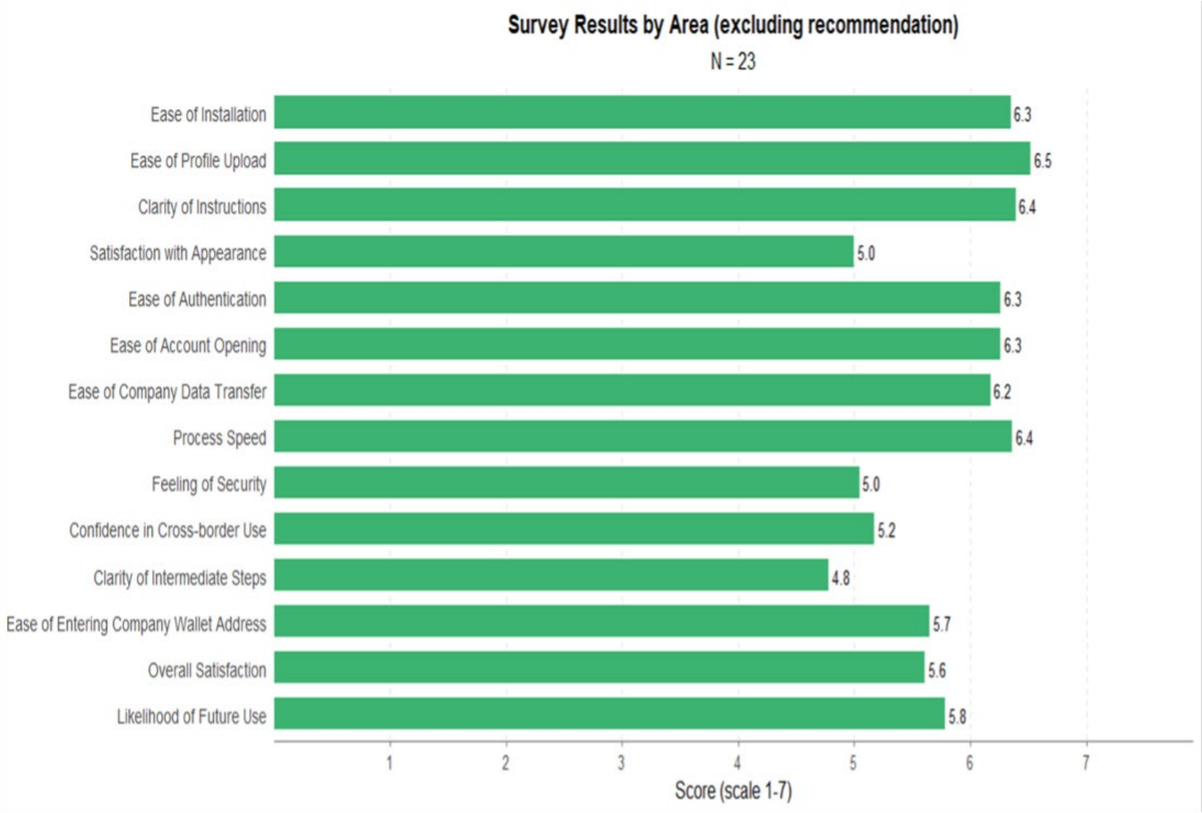


Figure 24 Survey results by area (KYC)

The feedback surveys (Figure 24) revealed that participants rated the onboarding process highly, appreciating the ease of application installation, profile creation, account opening, and authentication.

Instructions and process speed were also viewed positively. However, slightly lower ratings were observed in areas such as transferring company information, user interface design, overall satisfaction, and particularly user understanding of the steps involved, which received the lowest rating.

Users expressed moderate concerns about security and trustworthiness, indicating that despite technical reliability, the ease of the process sometimes resulted in uncertainty regarding security. However, this is generally typical in the industry, especially when banking applications and strong authentications are concerned.

Respondents recommended improvements such as clearer explanations of each step, multilingual support, and greater integration with other national platforms (e.g., vero.fi, suomi.fi). Enhancing transparency, especially around verification processes. Improving the visual appeal and usability of the interface were also identified as critical factors for future improvement.

4.4.4 Insights and lessons learnt

Schema

- At the time of deploying the pilot, there were no agreed schema definitions for LPID, EUCC, or PoA available in public repositories. First drafts were submitted in the EWC's repository during the pilot. The Implementing act on PIDs and the EU company law directive (Directive (EU) 2025/25) define the attestations only in high level, without the details of the syntax and semantics necessary for the implementation. No schema for LPID could be found in the Architecture and Reference framework (ARF).

- In particular, existing schemas lack proper formatting for specific attributes, such as a person's name or the "technical identifier" in the LPID.
- No detailed semantics definition exists for EUCC. For instance, in the schema delivered by Task 3.2, there is no definition for legal representatives' roles (e.g. "this person is a board member") and related constraints (e.g. "this person has the signature rights jointly with another board member").
- Tree structures (e.g., registered address in EUCC) are supported but lack advanced functionality. For instance, the relying party cannot currently request the user to present/disclose only those legal representatives who are board members or who can sign alone for the legal person.
- No detailed semantics definition exists for EUCC. For instance, in the EUCC schema delivered by Task 3.2, there is no definition for legal representatives' roles (e.g. "this person is a board member") and constraints (e.g. "this person has the signature rights jointly with another board member").
- The model of a PoA is incomplete. We adopted an approach where:
    - "Authorised signatories" are the persons registered as legal representatives in the business register and present in the EUCC. They have no scope and limitation in their powers. Therefore, these persons need no PoA.
    - "Persons with limited representation rights" are persons who are not registered as a legal representative in the national business register. To be able to represent the company, they need a PoA, which potentially contains a scope (what they can do e.g. "order parts") and a limitation (how much they can do e.g., "up to one million euros").
- The issuer of the PoA can be either the company itself or a trusted party (i.e. a QTSP).
    - We observe that in some countries (e.g. Hungary) a bank requires that a PoA is issued by a trusted party, such as, a notary. In eIDAS, we expect that means the PoA attestation must be issued by a QTSP.
- On the other hand, the legal person wallet itself could be used for issuing PoAs, enabling a simple procedure for the organisation to give mandates to its employees to act on behalf of the organisation. Issuing a PoA could rely on the sealing functionality of the legal person wallet. However, it is possible that issuing a PoA requires the organisation to register as a Trust Service Provider, increasing the administrative burden of the organisation and making the number of potential Trust Service Providers grow steeply. In practice, any holder of a legal person wallet could potentially be also a Trust Service Provider for PoA attestations. Therefore, it would be beneficial to seek for a way where an organisation can seal a PoA without registering as a Trust Service Provider
- PoA's "scope" is unclear. Will there be a pre-defined set of machine-readable scopes or will it be a free-text description of permissions for human eyes?
    - "This person is authorised to initiate payments"
    - "This person is authorised to open currency accounts"
    - "This person is authorised to sign contracts" with a limitation "up to 100.000 EUR"
- Schema sharing relies on non-scalable methods (e.g. sending schema definitions by email). Currently we have no fixed location where an authoritative schema version is maintained and shared. We expect the upcoming Implementing Acts on specifications and procedures for the catalogue of attributes (eIDAS Art 45e.2) to introduce a unified mechanism for this.

QEAA Issuance

- While (Q)EAA providers still pending, the process for issuing (Q)EAA for legal persons is still an unexplored territory and missing good practices that cover the specific needs of legal persons.
- Who is authorised to request a (Q)EAA for a legal person and what is the process? We can see that some attestations are public, and their process can be relaxed (for instance, extracts from the business register, such as an EU company certificate) while some attestations contain sensitive information (for instance, an ultimate beneficial owner certificate) and may need specific approvals in the requesting legal person side. We expect that the standards, specifications and procedures defined in eIDAS Art 45d-f (including the catalogue of attributes and attestation rulebooks) will define the necessary flow and approvals. ETSI 119 471 Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services (draft V0.0.11 (2024-11)) appears to have a related wording (REQ-EAASP-4.2.1-03: If the requested EAA Subject is not the EAA subscriber then the EEASP shall obtain and verify evidence (electronic or otherwise) that confirm the right to act on behalf of the EAA Subject.).
- How will the necessary transaction code (as defined in the OpenID for Verifiable Credential Issuance specification) for storing the attestation in the wallet be exchanged? The initialization of the issuance flow may have security risks, as the current issuance flow does not require a verification code.

Protocol limitations and incompatibilities

- Differences between (mobile and cloud) wallets raised concerns. We observed that wallets implement different protocols/profiles, such as the *did* or *redirect_uri* client id schemes, but only one at a time. For instance, when implementing the pilot, we found that Lissi implemented *redirect_uri* and iGrant.io did client id schemes (we learned they are planning to support multiple schemes). The credential needs to be issued and presented using the same client id scheme. This increases implementation effort for supporting multiple schemes. In the demo we implemented support for several client id schemes (*did* and *redirect_uri*) and the user was expected to select the one their wallet supports but we cannot expect real users to pay attention to this level of detail. The alternative is that the issuer and relying party take the burden to implement support for multiple protocols.
- In OID4VP, the credential presentation requests are limited to one credential of the same type at a time. It is not possible to request multiple instances or request "all" instances of a particular credential from the wallet.

Wallet implementation deficiencies

- In the pilot we observed different wallets implemented different OID4VP protocol version levels and, during the pilot, carried out backwards incompatible version updates, breaking the demo environment. For instance, if a wallet and RP used OID4VP draft version 19 and the wallet upgraded to version 20, our demo stopped working.
- It appears that current mobile wallets support only flat attestations and are lacking support for displaying attestations that have a hierarchical structure. This is problematic in particular for organisational attestations who have often hierarchical parts.

Co-funded by the European Union

- Support for a relying party requesting multiple attestations of different types (e.g. both LPID and EUCC) in a single presentation request is missing in several wallets.
- None of the wallet implementations we are aware of support selective presentation requests of hierarchical attributes. e.g. “I want you to present an EUCC attestation which discloses only those legal representatives who have the qualifier “can represent jointly”.
- The legal entity attestations (e.g., LPID, EUCC) can also be stored in and presented to a relying party from a mobile wallet. However, the mobile wallet may limit the way how the attestations can be presented. For instance, in a B2B scenario, the relying party may request the organisation to periodically present again their attestations to monitor any alarming changes. The user and relying party could agree that the relying party can request a new attestation any time and the mobile wallet presents it automatically, without disturbing the user with a manual process to scan a QR code etc. This is hardly possible if the mobile wallet does not expose to the Internet an interface to which the relying party could send the presentation requests, impeding the use of mobile wallets in B2B scenarios.

Relying Party

- No clear process is defined for a relying party to validate the attestation. In Appendix A of the 2nd iteration documentation, we propose a procedure with eight steps that a relying party needs to complete to accept a presentation from a wallet. This covers also cases where the issuer belongs to multiple federations/trust mechanisms. The exact validation process is use-case dependent, and the relying party needs to do what is necessary to adapt the process for its needs.
- The elliptic curve the issuer uses in the attestation signature must be supported by the verifier. Multiple elliptic curve variations need to be accounted for.
- In addition to using a relying party access certificate, a relying party should have an opportunity to present an LPID to authenticate to the wallet. This is particularly useful for relying parties who already have a legal person wallet (with LPID). Requiring a relying party to have two parallel authentication means (X.509 and LPID) is an unnecessary burden that hinders adoption. Furthermore, the relying party registration certificate could be implemented as an EAA that the Relying party registry has issued to the relying party’s legal person wallet which further presents it to the user’s wallet.
- When a natural person or legal entity presents data to a relying party, the relying party’s verifier component must be multi-protocol and flavour-agnostic (i.e. support all the options in the protocol). For instance, the user’s wallet may support multiple client id schemes (such as the *did* or *redirect_uri* client id schemes).

User Perspective

- As a user in this pilot, you manage two separate wallets: a personal wallet (for initial authentication) and an organizational wallet. Users often struggle to understand the distinction and functionality of each wallet, which can lead to a misunderstood experience.
- Explaining the concept of an organizational wallet to stakeholders proved challenging, primarily because personal wallets, used as a point of comparison, are not yet widely adopted or understood. This lack of familiarity with personal wallets made it harder to convey the distinct role and value of organizational wallets.
- In the pilot, we assumed a concept of eAddress (discussion paper available): the organisation representative typed the wallet’s address to a web form to enable the relying party to access the wallet. Controls need to be deployed for protecting the

eAddress endpoint, for instance, to avoid spam, anyone calling the wallet endpoint should first identify themselves (PID or relying party access certificate).

- When requesting presentation of attestations using the eAddress, the attestations were automatically presented without requiring explicit consent from the legal person. Users should have the opportunity to review and approve the data being requested before it is transmitted.
- During a demonstration to stakeholders, it was noted that presenting the LPID separately before the EUCC may be redundant. Since all relevant LPID data is included in the EUCC, users felt sharing the LPID as a distinct step was unnecessary (users did not know that LPID, unlike EUCC, has the feature of a device binding which protects against replay attacks).

Lessons learned in OpenID federation

- The verification process based solely on the information provided by the issuer (e.g., entity configuration retrieved from issuer's/well-known/openid-federation endpoint) is insufficient to establish trust. This is because the issuer can be a member of several federations i.e. the relying party may be able to construct several parallel entity statement paths to it and those paths may have different/conflicting policies covering e.g. the issuers liability on damages it has caused.
- To avoid policy ambiguity, the issuer should clearly indicate the policies and trust framework used for issuing the credential along. We propose this information is included in the credential itself, not just in the entity statements fetched from the OID federation trust infrastructure. Consider including the complete path of entity statements to the attestation itself?
- The issuer onboarding process is a governance topic that needs clarification in the trust framework. A proposed solution is outlined:
    - The onboarding process requires the registrar (the parent node in the OID federation hierarchy) to specify the issuer's identification (e.g. EUID).
    - If the federation covers multiple attestation types (attestation schemas), the registrar must indicate the attestation types the issuer is authorised to issue (e.g. the issuer is good to issue EUCC attestations but not tax debt certificates). This information could be included to the subordinate entity statements.
- Additionally, the liability associated with the issuer needs to be specified, potentially using the subordinate entity statements.

4.4.5 Recommendations

- Work on the standardisation of LPID and EUCC schemas.
- Further work on the PoA model definition and scope, and on the requirements for PoA issuers and pilot PoA in different business scenarios.
- Introduce in the Implementing Acts on specifications and procedures for the catalogue of attributes a unified mechanism for the maintenance and sharing of schema versions.
- Work on the process for issuing (Q)EAA for legal persons and develop good practices that cover the specific needs of legal persons.
- Further work on the concept of the business wallet, legal binding and on protocol limitations and deficiencies across different wallets and multiple client id schemes.
- Work on the elaboration of hierarchical structured attestations and automated presentation upon request.
- Have stable and mature specifications, as interop testing gets very challenging with different versions of specifications.

- Work on educating and explaining to the users the role of natural person and business wallets and how the business wallet comes to complement functionalities of the natural person wallet in the business processes and transactions.
- Further work on the trust framework.

4.5 P4.1.1 KYS 2.0 Peppol network registration and use

4.5.1 Assessment summary

The following tables provide an overall assessment of the pilot. The first table evaluates the pilot's performance against its own defined goals, while the second assesses the extent to which the pilot achieved its intended ambition level.

Table 15 P4.1.1 own goals evaluation table

Goal Description	Rate (1-5)*	Comments
1. Enable end-user registration with Peppol Service Providers via EUDI Wallet	3	The registration flow was successfully implemented in the test environment, showing that identity-based onboarding to a service provider (e.g., B2Brouter) is feasible using the EUDI Wallet.
2. Enable end-user identification directly via the EUDI Wallet or via service providers	4	The pilot clearly demonstrated how identification can occur securely through the EUDI Wallet. Verified identity attributes were successfully shared with the platform as intended
3. Verify end-users as trusted receivers in the Peppol network	3	The concept for automated verification of organizations as trusted Peppol participants was successfully validated in the testing environment, with business logic and attribute handling implemented as specified.
4. Enable authenticity proof and automated provision of company master data through EUDI Wallet	4	The solution allowed automatic transfer of verified company data (e.g., legal name, VAT, IBAN) from the EUDI Wallet to the platform, reducing manual data entry and enhancing trust.
5. Provide automated service contract generation and Peppol activation	3	After identity verification, the pilot enabled automated generation of a digital service contract and onboarding logic for Peppol services, demonstrating feasibility in a test scenario.
6. Enhance Peppol registration process to be faster, more reliable, and user-friendly	3	The pilot successfully simplified the onboarding experience and showed potential for improved user experience and administrative efficiency in a controlled test setup.

***(Rates from 1 = not achieved to 5= fully achieved or N/A = Not Applicable, Not Available)**

Context and Constraints: The pilot successfully implemented and tested an innovative solution for onboarding organizations to the Peppol network using verified identity attributes provided through the EUDI Wallet. While the technical integration and process design were validated in a controlled environment, the transition from test to production could not be completed due to the unavailability of the original EUDI Wallet provider Archipels, whose services were discontinued during the project lifecycle. Despite this, the pilot demonstrated a viable and replicable approach that can be adapted with alternative providers in the future.

Table 16 P4.1.1 evaluation on ambition level achievement

KPI	Target planned within pilot	Achieved	Please specify names of the achieved KPIs	Comment: if your commitment differs from the initially planned (D3.5), explain why
Number of wallet issuing countries	5* TBC	1	France	
Number of ODI issuing countries	5* TBC	1	France	
QEAA (PubEAAs)	-	1	Infogreffe	
Number of relying parties	1	1	B2Brouter	
QTSP providers		1	Archipels	(Note: the operations and solution provided by Archipels were discontinued during the project lifetime)
Wallet users (legal persons)	5* TBC	-	Potentially every user of B2Brouter can use the service. However, so far it has not been possible to find production use cases with real users and/or companies and to execute live transactions. The pilot was only executed with test accounts.	
Wallet users (natural persons)		-	To verify legal persons, natural persons must also authenticate with their wallet to approve their mandate to act on behalf of the legal person.	
Number of transactions completed		-	Only test	
Number of qualified signatures issued		-	Only test	
Number of ODI credentials shared		-	Only test	

4.5.2 Pilot execution in production environment

The systems involved in the pilot were either existing platforms used in live operations or newly adapted components built on top of production-ready infrastructure.

The B2Brouter platform used in the pilot was deployed in a pre-production environment, which mirrors the production configuration in terms of architecture, workflows, and business logic. This allowed for a realistic test scenario while avoiding risks to live data and operations.

Co-funded by
the European Union

The EUDI Wallet integration was enabled through Archipels, acting as a QTSP (Qualified Trust Service Provider). This component also operated in a pre-production setup during the pilot with Infogreffe connected as QEAA. While the pilot progressed effectively under these conditions, Archipels' services were discontinued during the pilot period, which prevented the transition to a production rollout.

Table 17 P4.1.1 execution context

Name of the system	Production	Pre-production /acceptance	Clone of production built for the pilot	New prototype built for the pilot
B2Brouter platform (Relying Party)		X		
Archipels (QTSP provider)		X		
Infogreffe (QEAA)		X		

4.5.3 Pilot user testing feedback

In the context of the KYS Peppol network registration and use pilot, no formal user testing involving external end-users was executed. As the pilot remained in a pre-production environment and did not transition into live operation, it was not feasible to conduct structured user testing sessions or gather user feedback from actual platform participants.

Accordingly, no questionnaire was developed or administered during the course of the pilot, and no user testing results are available.

4.5.4 Insights and lessons learnt

Implementation and Integration

One of the key takeaways from the pilot implementation of Archipels' digital identity wallet is that the API integration process was relatively straightforward. The solution is well-structured and allows for easy implementation within existing business workflows. From a technical standpoint, the ability to quickly integrate and verify identities using KBIS attestations from Infogreffe showcases the usability of Archipels within the French market. The initial deployment was completed within the expected timeframe, indicating that the readiness of the technology is promising.

Availability of Attestations and Geographic Expansion

While Archipels already supports specific use cases, such as KBIS attestations in France, the current solution does not (yet) provide a broad range of Qualified Electronic Attestations of Attributes (QEAA) across different jurisdictions. This presents a limitation for global operators like B2Brouter, whose customers span multiple countries. To fully leverage the solution, additional attestations from other regions will need to be incorporated. This highlights the necessity for expanding partnerships with authentic sources beyond Infogreffe to ensure comprehensive cross-border verification capabilities.

User Onboarding Challenges

One of the major hurdles identified is the limited adoption and awareness of EUDI wallets. User onboarding is not as seamless as expected, largely due to the fact that digital identity wallets are not yet widely known or used. The challenge lies in encouraging businesses to

Co-funded by
the European Union

adopt this new paradigm for digital identity management. To mitigate this, the project should focus on targeted user engagement strategies, including onboarding early adopters from within the consortium to create an initial user base willing to test and refine the solution. So far it has not been possible to find production use cases with real users and/or companies and to execute live transactions.

Interoperability Considerations

Another critical aspect that requires further validation is the interoperability of the solution when users and verifiers operate with distinct EUDI wallet providers. The solution currently works well within the Archipels rather French ecosystem, but its effectiveness in heterogeneous environments is yet to be determined. This presents a risk that the system may not function as expected when different EUDI wallet solutions from different countries interact. Moving forward, controlled testing scenarios should be designed to identify gaps in standardization and evidence verification across multiple providers.

Standardization and Rulebook Harmonization as the Baseline for Interoperability

Experience shows that true interoperability depends on widely accepted, harmonized rulebooks rather than project-specific solutions. While pragmatic, custom rulebooks have enabled quick progress, they fall short of addressing the consistent needs of (Q)EAAs, QTSPs, and relying parties across jurisdictions.

To ensure reliable, scalable, and cross-border use, standards must be defined at the European level and aligned with real-world administrative and business processes. Local legal and procedural differences—such as varying proof or data requirements—highlight the need for this harmonization.

This challenge is not unique to EUDI Wallets but is also seen in initiatives like eProcurement and OOTS. Without agreed, domain-specific rulebooks and data models, interoperability remains limited, regardless of how technically sound the infrastructure may be.

Managing mandates and legal representation in EUDI Wallets

The process of verifying legal entities and managing mandates through EUDI Wallets introduces significant complexity for end users. In scenarios where a user must act on behalf of a company, multiple conditions must be met. Both the legal entity and the authorized person need established wallets; a valid mandate linking them must exist; and the attestation process must follow a specific sequence involving third-party services such as Archipels and national identifiers like the SIREN number. The user must not only identify the company but also select the appropriate organizational wallet and connect their own personal wallet to complete the process. While technically sound, this workflow can be difficult to navigate, particularly for non-expert users, and any missing element—such as an unestablished wallet or undefined mandate—can cause the process to fail. To ensure adoption, the EUDI Wallet ecosystem must prioritize usability, clear guidance, and simplified mandate management for interactions between natural persons and legal entities.

Conclusion

While the initial implementation of Archipels' digital identity wallet has proven its technical feasibility and ease of integration, significant challenges remain to achieve widespread adoption and true interoperability. Expanding the range of Qualified Electronic Attestations across multiple jurisdictions is essential to support diverse use cases and global operators like B2Brouter. Moreover, increasing user onboarding and awareness is critical to foster real-world adoption.

Equally important is the need for standardized, harmonized rulebooks and data models that are accepted and implemented consistently by Qualified Trust Service Providers (QTSPs) and relying parties across Europe. The pilot demonstrated that project-specific rulebooks, while pragmatic for initial testing, do not sufficiently address the complex, cross-border realities of digital identity verification. Without coordinated efforts by domain-specific expert groups to align legal and administrative requirements, interoperability will continue to face significant hurdles—even if the underlying technical infrastructure is robust.

Managing mandates and legal representation in EUDI Wallets also presents a major usability challenge. When a user must act on behalf of a legal entity, multiple conditions must be fulfilled—such as the presence of both organizational and personal wallets, valid digital mandates, and a clear authorization flow. As demonstrated in the pilot, the current process is difficult to navigate and prone to failure if even one element is missing. Simplifying this workflow and ensuring user-friendly mandate management will be crucial for enabling seamless interactions between natural persons and legal entities.

These insights will guide future efforts to refine onboarding processes, broaden geographic applicability, and ensure seamless compatibility among different EUDI Wallet providers. Ultimately, addressing both technical and standardization challenges is vital to realizing a scalable, secure, and interoperable identity verification ecosystem that supports trusted digital transactions across Europe.

4.5.5 Recommendations

- Expanding partnerships with authentic sources in different countries to ensure comprehensive cross-border verification capabilities.
- Educate businesses to adopt the new paradigm for digital identity management, focus on targeted user awareness and engagement strategies, including onboarding early adopters to create an initial user base willing to pilot and further refine the solution.
- Ensure that wallet provider solutions from different countries are interoperable.
- Work further on standardised, harmonized domain-specific rulebooks and data models addressing the consistent needs of (Q)EAAs, QTSPs, and relying parties across different European jurisdictions in order to support diverse use cases and global operators.
- Coordinate efforts by domain-specific expert groups to align legal and administrative requirements, e.g. align with public procurement and Once Only Technical System (OOTS).
- Work further on usability, clear guidance, and simplified mandate management for interactions between natural persons and legal entities for fostering real-world adoption.

4.6 P4.2.1 Verifiable eReceipt

4.6.1 Assessment summary

The following tables provide an overall assessment of the pilot. The first table evaluates the pilot's performance against its own defined goals, while the second assesses the extent to which the pilot achieved its intended ambition level.

Co-funded by the European Union

Table 18 P4.1.1 own goals evaluation table

Goal Description	Rate (1-5)*	Comments
A person can get a structured and verifiable digital receipt (aka vReceipt) for their purchase and pass it to the accounting/financial management system for downstream consumption.	4	We managed to demonstrate issuing of vReceipt together with WP2. We also demonstrated how vReceipt can be presented to a relying party, but didn't manage to attract a travel expense/cost management service provider to integrate them to their service.
A person can request automatic delivery to an employer system (e.g. expense management)	3	We demonstrated how vReceipt can be delivered also to the employer's legal person wallet, but that was not part of the pilot with WP2.
Efficient negotiation method	4	We presented our suggestion for an engagement protocol to the EWC community (in the EWC Friday tech talk) but found that in the project there was no wider interest in studying a mechanism for negotiating different ways to deliver a vReceipt. Instead, we started to study an approach where the vReceipt issuance was integrated to the EUDIW payment flow, resulting to the approach proposed in RFC-011.
Compound proofs (or other method of proving VAT through vReceipt) Archival of proofs (self-contained proving)	1	We didn't make progress in attaching the seller's VAT attestation to the vReceipt. This was in particular because the ARF does not assume issuers (here: sellers) to have a wallet of their own.

***(Rates from 1 = not achieved to 5= fully achieved or N/A = Not Applicable, Not Available)**

Table 19 P4.2.1 evaluation on ambition level achievement

KPI	Target planned within pilot	Achieved	Please specify names of the achieved KPIs	Comment: if your commitment differs from the initially planned (D3.5), explain why
Number of wallet issuing countries	3	1	Sweden (IGrant.io)	Due to the requirement of the pilot to be a production service with production payments it was necessary to enroll the wallet in Banka Transilvania. Banka Transilvania

				could only support this feature with iGrant.io wallet.
Number of ODI issuing countries	0	0	No ODI credentials in this pilot	
QEAA (PubEAAs)	0	0	No QEAA issued in the pilot	
Number of relying parties	1	3	vreceipt.minisuomi.fi Fast Ferries via UAegean	Originally, we envisioned a single relying party to verify the vReceipt. As the pilot scaled into a production service, the model expanded: Fast Ferries became a second relying party—issuing the vReceipt and initiating the payment request while consuming PID, PhotoID, and StudentID credentials—while Banka Transilvania acted as a relying party responsible for verifying the payment authorization
QTSP providers	0	0	No QTSP in this pilot	
Wallet users (legal persons)	0	0	vReceipts are issued primarily to the wallets of natural persons (travellers)	
Wallet users (natural persons)	100	12	vReceipts issued to natural person wallets in production	The pilot evolved from a concept trial into a production-grade service handling real payments and receipts. That transition introduced unanticipated

				constraints: all participants had to be Banka Transilvania customers and possess an active Romanian passport. Although hundreds of vReceipts were issued to natural-person wallets in pre-production, the standout achievement is the successful execution of live transactions in production.
Number of transactions completed	100	12		12 in production and more than 100 during pre-production tests (please see above)
Number of qualified signatures issued	0	0	No QES in this pilot	
Number of ODI credentials shared	0	0	No ODI credentials in this pilot	

4.6.2 Pilot execution in production environment

The vReceipt test was created together with Cyclades Fast Ferries (CFF) beneficiary. CFF's ticket-issuing platform is already live in production (in other words the pilot is executed in a production environment with real tickets being issued and real payments being authorised by the EUDI Wallet). The only enhancement still outstanding is the application of a qualified electronic signature to boarding passes and eReceipts – a step needed solely to satisfy cross-domain trust-framework requirements when third parties wish to rely on the documents. Once that signature layer is added, any EU citizen could use the service provided two further conditions are met:

I. their EUDI Wallet can be linked to a payment instrument issued by any EU bank, and
II. those banks recognise and accept merchant-initiated authentication flows originating from the EUDI Wallet

Table 20 P4.2.1 execution context

Name of the system	Production	Pre-production /acceptance	Clone of production built for the pilot	New prototype built for the pilot
Issuer of vReceipt	X			

Receiver of vReceipt				X

4.6.3 Pilot user testing feedback

The pilot set out to verify whether the EUDI Wallet can deliver a faster, more trusted ferry-ticket checkout than current web or in-app card flows, combining payment with receipt and boarding pass issuance. Participants evaluated only the purchase journey – wallet provisioning and ID enrolment were out of scope. Using an 18-item questionnaire (with 5-point scales, semantic comparisons, free text, and 0–10 NPS), respondents generally reported high ease and clarity: start-payment ease averaged 4.0.

Perceptions of value versus the “normal” checkout were strongly positive. Sixty percent called the overall experience and ease “considerably better,” and an equal share rated privacy and perceived security substantially higher. Trust carried across contexts: 60% “completely trust” the wallet for small and large purchases and when a site requires proof. Speed perceptions were more mixed (20% faster, 20% slower). Nevertheless, advocacy is strong, with an average NPS of 8.8 and a reported +75 score (although the number of pilot users was limited). Furthermore, participants appreciated the fact that using the wallet they have “all their documents in one place - including receipts” and that they only have to use the wallet to introduce all required data by the merchant and authorize the payment.

Friction points cluster around avoidable repetition and edge-case handling. Two users mentioned having to re-type card details, undermining the “fast checkout” promise. Error messaging scored lowest (3.8, with 20% bottom-box), and one user hit blocking bugs (a hang at step 6 and a missing receipt), threatening trust if unaddressed.

4.6.4 Insights and lessons learnt

Early on we saw that the vReceipt pilot overlapped heavily with WP2’s travel-payment scenarios. In spring 2024 the T3.3 team therefore teamed up with WP2 – specifically the UAegean group leading the Fast Ferries use-case, where passengers receive ferry tickets as attestations in their mobile wallets. We formed a joint working group to:

- draft the technical specifications for vReceipt issuance, and
- design and build the infrastructure for a unified pilot flow.

Combining the pilots produced a single, end-to-end experience that covers ticket purchase, payment, and the automatic delivery of a verifiable receipt – the natural conclusion of any transaction. Sharing both the user base and the UX has already yielded richer feedback for the overall programme.

Usability is crucial for issuing vReceipt – if receiving a vReceipt is clumsy, buyers don’t bother to have one. A major breakthrough was done late 2024 by the University of Aegean and iGrant.io who discovered how a payment can be done and vReceipt issued in a single transaction. The approach is documented in RFC011 and implemented for the Phase 3 piloting.

The ARF is currently focused on issuing attestations to natural person wallets who then present them to relying parties. In particular, issuers (or relying parties) themselves are not supposed to have a wallet (with attestations describing their holder). For vReceipt, we can see value for a setup where also the issuer (seller) has a wallet and can attach to the vReceipt their own attestations, in particular a VAT attestation (issued to the seller by a competent tax administration) that confirms the seller’s VAT number. Unfortunately, we were not able to focus on this kind of "chained attestation" in the pilot and are not aware of any related work. In upcoming projects, attention should be paid to how the issuer can attach their own VAT attestation to the vReceipt they issue. The receiver of the vReceipt could then use the attached VAT attestation to ensure their right to deduct the purchase's VAT in their own VAT declaration.

4.6.5 Recommendations

- Work on the enhancement of the definition of the business wallet, ebnabling also the issuer having a wallet.

4.7 P4.3.1 Create a company branch in another country

4.7.1 Assessment summary

The following tables provide an overall assessment of the pilot. The first table evaluates the pilot's performance against its own defined goals, while the second assesses the extent to which the pilot achieved its intended ambition level.

The pilot goals defined in D3.5 were to verify hypothesis 1, statement 1-3 and hypothesis 2. It was optional to also verify statement 4 in hypothesis 1.

Table 21 P4.3.1 own goals evaluation table

Goal Description	Rate (1-5)*	Comments
The wallet can be used for authentication	3	The business wallet can be used for mutual authentication with the LPID as described in RFC-005. This part has been achieved. However, we have not achieved to implement a login solution for login of a representative with their NPID attestation. This is something we will have to continue working on in the next pilot
The wallet can be used for signing	1	The wallet can't be used for signing. If we had had an available remote signing service, we would want to have tried this as well, but to our knowledge there was non-available. The standards for signing with a wallet had not been written either.
The wallet can present attestations to a relying party	4	A EUDIW has been successfully used to present attestations to Bolagsverket and Brønnøysundregistrene. We have done this initiated from our eServices via QR-code. We could also try the authorization flow and have the same process initiated by an EUDIW, but we did not have the time to test this as well.
The EUDIW for a RP can be used for accepting presented attestations and use them in internal business processes	4	The EUDIW for a RP (Bolagsverket and Brønnøysundregistrene) has been used for accepting and presenting attestations in internal processes. We could have connected some more of these internal processes to the business wallet, such as for registering of cases, but this is something we can add in upcoming pilots.

***(Rates from 1 = not achieved to 5= fully achieved or N/A = Not Applicable, Not Available)**

Overall, most hypothesis goals have been fulfilled in a satisfactory manner, except for the signing functionality which could not be tested. This was not due to the pilot, but to missing external support functions for signing functionality.

Table 22 P4.3.1 evaluation on ambition level achievement

KPI	Target planned within pilot	Achieved	Please specify names of the achieved KPIs	Comment: if your commitment differs from the initially planned (D3.5), explain why
Number of wallet issuing countries	2	2	Sweden, Norway	
Number of ODI issuing countries	2	2	Sweden, Norway	
QEAA (PubEAAs)	3	3	EUCC, NPID, LPID	
Number of relying parties	2	2	BRREG, Bolagsverket	
QTSP providers	0	0	None	
Wallet users (legal persons)	2	2	BREEG, Bolagsverket	
Wallet users (natural persons)	15	15	Test persons from Norway and Sweden	
Number of transactions completed	50	150	BREEG and Bolagsverket combined	
Number of qualified signatures issued	0	0	None	
Number of ODI credentials shared	40	80	EUCC, LPID, NPID	

4.7.2 Pilot execution in production environment

Our pilot did not run in a production environment. We built a prototype of a new e-service "Create company branch" with only test data and no real-life integrations against our systems except for fetching some test data.

Table 23 P4.3.1 execution context

Name of the system	Productio n	Pre-production /acceptance	Clone of production built for the pilot	New prototype built for the pilot
eService				X

The number of transactions performed was 150.

4.7.3 Pilot user testing feedback

The following section summarises the main user test results, key findings and considerations. For more details of the user testing, such as questionnaire, target group and implementation of the tests and detailed results, please refer to ***Annex B: Create a company branch – Testing***.

Even though users struggled a bit in understanding the concept of digital identity wallets and the toggling between different sites, countries and devices, there were a lot of positive reactions to this new process. Users considered that the registration is not difficult anymore, it is much better and efficient, and they only need to know what credentials need to be shared in order to do the process of creating a branch. They also considered the flow more secure, as everyone needs to identify themselves.

The key findings and considerations include:

- Visualisation of expectations and help the user understand what to do and where they are in the process, and whether they have done the right thing in each step is key for success.
- Maintain an EU-centralised common page that collects all necessary web addresses for the different issuing processes for each use-case/attestation.
- The “create company branch registration” process is better and more secure with using digital attestations than paper-attestations and registration form on paper, leading to better data quality in registers, reduction of case handling time, simplification of the process allowing more people to handle it without extensive training or experience compared with today. Even the consultants helping clients today could envision a service where the client did this process themselves.
- There is a strong need for plain language making it easier for users to understand the terms, their meanings, and what data was being shared with whom. Language and abbreviations are seen as cryptical for people with no experience from the terminology.
- The overall concept of digital wallets, proofs, and trust infrastructure is difficult to grasp. Some of the users reacted negatively and thought that authorities should handle and that there should be a common European registry that contains all relevant data from every national registering authority. Others perceived the attestations as just a pdf, being though happy to have moved away from paper. They did not understand the trust infrastructure behind the attestations. And this emphasises more the importance of adoption and envisioning the value behind the identity wallet technology in a clear and precise way.

4.7.4 Insights and lessons learnt

A. Technical challenges and insights

1. Lifecycle management of attestations

a. Revocation

Revocation is a necessary feature; without it there is no way to make an attestation invalid before an expiry date has passed. There are many mechanisms for handling revocation. Each revocation mechanism has different properties. During EWC we have piloted status lists according to the JWT status list standard. It gives a good balance between, ease of implementation, ease of understanding and privacy.

Using short lived attestations as a way to remove the need for revocations does not seem like a reasonable approach for LPIDs and EUCCs that we are issuing. This approach would put a significant stress on the issuer and holder. Issuers would need to issue several million attestations every day. Holders would need to be in constant contact with issuers. Since wallets for individuals according to the ARF are phone-based this would also make the receiving of attestations difficult in areas with little or no cellular coverage or areas with congested cellular traffic.

Additionally, the following use-cases are currently not covered:

I. A holder deleting an issued attestation (currently no report back to issuer about deletion).
II. No defined/discussed way of a verifier to report suspected misuse of an attestation (for example in case of theft of the wallet/credential). All parties involved in the attestation exchange should have a way to report/signal suspicious behaviour

b. Expiration

No specific tests were done with regards to expiration of attestations. A couple of points that need to be further analysed include: i) Validity period of attestations is currently undefined. Valid time periods per attestation should be standardized along with its schema, and ii) Some attestation formats like SD-JWT have expiration (exp) and issuing time (iat) attributes in their standard. The metadata for EUCC and LPID have these as well. How this overlap is handled must be decided. SD-JWT and JWTs are automatically seen as invalid outside these timestamps.

c. Re-issuing

Reissuing has not been tested. There have been discussions on how this should be done. This needs to be investigated further. Current definitions say reissuance is initiated from the holder, however on change of values (company name change or signatory rights in an LPID or EUCC respectively) the reissuance should be able to be triggered by the issuer (ARF 6.6.2.1). The OpenID4VCI standard has the concept of refresh tokens, so there is the question of whether these are seen as good enough to reissue a LPID. The reissuance process needs to be the same for a certain type of attestation in the entire ecosystem.

2. How to handle “Lost” wallets

Based on the ARF used in EWC, the discussion of recovering lost wallets or disabling lost wallets is not discussed sufficiently. There is a requirement for PIDs to be revoked when the Wallet Unit Attestation (WUA) is deleted from the wallet. The expectations for the timeline of this revocation should be clarified (check hourly/daily/weekly?). it is assumed that this will also be valid for LPIDs. (ARF 6.6.2.4). Due to the nature of the LoA “high” for PIDs and LPIDs, such a process should be described, and assigned to the countries’ issuance instance. Possibly with a “revoke and re-issue” to a new wallet only. A user journey of what can happen to a wallet should be mapped out, and technical processes to support that journey should be defined.

3. SDKs, and format agnostics integrations

The requirements of supporting multiple attestation formats have quickly been shown to offer challenges. With two international parties, and three additional Norwegian national parties involved, multiple different formats where implemented. As the presentation definition of OpenID4VC requires the definition of a format to request, this led quickly to incompatibility and required rewriting to the same attestation format.

Requiring a user to tell us who issued an attestation, to then look up what format to request the attestation on, makes the system overly complicated, once you have more than one attestation in an exchange and places a significant cognitive load on the wallet user. This pattern would also require the document format to be published centrally.

Disconnecting the credential format from the attestation definition request would be preferable. If this problem is not solved through a SDK, intermediary, or in the protocol itself, the impact on the user experience, and therefore adoption rate is assumed to be significant.

4. Integration through wallets or directly over OpenID4VC

The choice of using a vendor for our part of EWC, was built on the assumption that a wallet vendor would work well as an abstraction layer for the OpenID4vc protocol, and inter-ecosystem communication. The value of this approach has been validated in our use case. A wallet vendor change was done part way through the project. Slight differences in the APIs between vendors lead to minor changes, that could follow well established IT process patterns, enabling fast on and off boarding of personnel, and a lowered overhead cost. While this cost would not have been incurred by using the OpenID4VC protocol directly, the increased complexity and unfamiliarity of the OpenID4VC protocol would have incurred an overall higher cost. Especially for smaller teams and enterprises. This might change with the maturity and development of SDKs.

5. Is OpenID Connect a good protocol to use for Legal Person wallets?

A general question should be raised about the OpenID4VC protocol in general in regards to legal person wallets as the main standard. For organizational wallets we see a need for server-to-server communication without the need for human interaction. This has not been fully validated to work with OpenID4VCI/VP protocols. This is largely because there has not been any prioritized use case that requires this.

6. Schemas-version control, information governance, joint definitions, version changes, how do we re-issue?

During the EWC work, one thing was a recurring issue, which will also be prevalent going forward. The change of schemas, and information governance. While changes in schema in pilots occur regularly in a pilot phase, they should also be accounted for in the operational phase. Should a new schema version lead to re-issuing and consequently revocation of all previous attestations with the old schema? In such a case, a mechanism for this should be defined. The change of potentially required information means the re-issuance process initiated by the holding wallet would fail in our use-case, as the re-issuance with the same data content is planned handled by our wallet vendor, which will fail with changing data.

There is also potentially a need for more data-governance work, or at least a framework to expand the EUCC with more information, potentially country specific. Some of our currently observed problems of insufficient data for legal validity might be addressed by the Power of Attorney and Signatory Rights work planned in the next LSP WE BUILD.

B. Legal insights

Fundamental legal interpretations remain unclear, particularly regarding the nature of LPID attributes proposed in CIR 2024/2977. For example, it remains uncertain whether PID providers can select which amongst the five different organizational ID to issue and whether wallets must support all organizational IDs proposed in the Implementing Act.

The European Unique Identifier (EUID) as a common European identifier was introduced by Directive 2012/17/EU regarding the establishment of the Business Registers Interconnection System (BRIS). The EUID was a necessary prerequisite for member states to be able to connect their national Business register(s) with the European Central Platform.

The EUID is structured with the prefixes of the country code and register code in addition to the company registration number. In BRIS, there are procedures to handle the affected EUIDs due to transfers between national registers and changes in national register structure. Updated core information and status on entities covered by the Company law directive is available to the public via the e-Justice portal.

With the establishment of BORIS, the scope of EUID was expanded as member states were required to connect their national Beneficial Ownership Registers via the European Central Platform. BORIS covers not only limited and commercial companies, but also other legal entities, trust or similar arrangements. Necessary measures and requirements to ensure uniform conditions for connection with the European Central Platform were given in the Commission implementing regulation (EU) 2021/369. The relationship of national registration number with the European Unique Identifier and company registration number is regulated in point 3.1 inn Annex to Article 1:

“The beneficial ownership register shall share with the European Central Platform the national registration number and, for companies, the European Unique Identifier (‘EUID’) attributed to them in the Business Registers Interconnection System (‘BRIS’) as well as the company registration number, in case the latter is different from the national registration number. The company registration number shall be used to attribute the EUID to companies that do not have an EUID in BRIS. For other legal entities, trusts or similar arrangements, the EUID shall be attributed based on the national registration number.”

The extended use of EUID has not resulted in increased requirements to publish updated core information and status information about legal entities that is not covered by BRIS in the e-Justice portal.

EUID seems to be the best company identifier to use with the LPID. But it will require a more harmonised regulation between company law, beneficial ownership and Digital Identity Wallet / European Business Wallet.

Topics to discuss:

- Should updated core information and status information for all entities with EUID be publicly available through BRIS.
- Should a harmonised form of Registration Certificate be available for entities with EUID that is not covered by the Company law directive. And should this Certificate also be compatible with the European Digital Identity Wallet,
- Issuing EUID to entities in public sector?
- Issuing EUID to sole traders operating under organizational ID?
- LoA High requires strong authentication, but re-issuance of LPIDs is proposed without user action in some cases and it is therefore unclear if this fulfils LoA High.
- At both the national and organizational levels, further analysis is needed to determine which representatives are authorized to apply for and sign the application for an LPID, which organizational statuses qualify for LPID issuance, and which attestations should be provided in a format compatible with EUDIWs. Necessary controls for LPID issuance on Level High should be standardized across EU/European Economic Area (EEA).
- It remains to be analysed which laws need to be adapted on a national level to be able to issue attestations (including LPID) fully digitally.
- Further exploration is needed to determine how and whether the same integrity and data protection requirements, such as pseudonyms, anonymity, data minimization, selective disclosure, and collusion tracking, apply to organizational data and use cases.
- Presentations received by a wallet might challenge known and accepted patterns for when a document is considered received by the governmental body in Sweden. (Can „eget utrymme“ be used in conjunction with the wallet? When is a presentation considered an „inkommen handling“?)

Co-funded by
the European Union

- The "European Business Wallet" was introduced in the "Competitiveness Compass" in January 2025 and was followed up in the Commission work program for 2025. The Commission will by the end of the year propose a new regulation for "European Business Wallet" (EUBW). Very little is known about the EUBW initiative at present time, and it is not clear how it will relate to "European Digital Identity Wallet" (EUDIW) regulation. From a legal perspective the new initiative has created quite more of uncertainty for the time being.

C. Business learnings

In the following paragraphs, learnings from the Business registry perspective regarding the impact of the regulation on daily business operations are described, as well as the feedback on adoption that business registries have received from businesses in Nordic countries during the EWC pilot, and why the EUID is an important identifier for business registries.

1. Insights and Use

The Create Branch pilot revealed several critical insights that should guide the future development and deployment of digital wallets for business use. Business registries, in particular, face both significant challenges and promising opportunities when it comes to issuing and utilizing digital credentials.

One key opportunity lies in reducing lead times – an immediate and highly valuable benefit for both businesses and registries. However, the greatest long-term impact stems from improving data quality. Higher quality data builds trust, and trust is essential for achieving broad ecosystem adoption.

During the Create Branch pilot, several areas of significant value creation were observed:

- **Reducing errors and registry support needs:** Simplifying the application process for users led to fewer mistakes and misunderstandings when completing forms. This, in turn, reduced the need for registry support, returning fewer applications for correction and saving valuable processing time.
- **Automation of business registry processes:** Automated processing dramatically decreased case officer workload. Since much of the processing time involves source verification, the ability to validate trusted digital credentials reduced the manual burden. In some cases, full automation became feasible, freeing up further resources.
- **Establishing a single source of truth:** Having a single, authoritative source for critical data – and a unified mechanism for updating it – enhanced trust in the information. Improved data trust translates into higher overall data quality, which is particularly valuable in scenarios like international trade and cross-border business activities.
- **Standardized data across the EU:** The adoption of standardized European credentials and harmonized systems across Member States significantly increased trust and efficiency. With trusted, standardized data, manual checks became less necessary, further speeding up processes and creating more value for all stakeholders.

These findings illustrate how digital wallets, when properly integrated with trusted registries, can drive both operational efficiency and systemic improvements in data integrity.

2. Implications of regulation (EU) 2024/1183 for Business Registries and the Need for Shared Infrastructure

The requirements introduced by eIDAS 2.0 have far-reaching consequences for the digital services provided by business registries. During the analysis of the "Create company branch" use case, it has become clear that a broad range of existing systems must undergo significant adaptations. This includes login and authentication services, signing services—often governed by long-term contracts with third-party providers—and all registration-related e-services. These systems will need to support new formats such as Verifiable Credentials (VC) and mDOC. Similarly, services responsible for issuing official information must be upgraded to enable issuance in these new formats.

A further implication is that public authorities responsible for maintaining registers will likely need to issue attestations, effectively taking on the role of trust service providers. This comes with additional regulatory obligations, including compliance with organisational and technical security standards and supervision frameworks.

Crucially, each individual agency across EU Member States will need to carry out these adaptations independently, representing a considerable cost to society. To reduce duplication of effort and promote interoperability, there is a clear need for commonly available, open-source components that can be reused across agencies and Member States. Even more beneficial would be a model in which such components – such as modules for issuance, login, digital signing, verification and validation, and revocation – are developed or provided per country, under public ownership or coordination, and made securely accessible to all relevant authorities.

3. Adoption of wallets in Nordic countries

The societal costs outlined in the previous paragraph can only be justified if there is broad adoption of digital wallets across Europe. Achieving this level of uptake requires that the wallet model supports not only individuals, but also businesses. Feedback from participating companies in the EWC pilot has clearly indicated the importance of enabling organisations to use wallets for their business transactions – whether with other companies, individuals, or public authorities – across the EU.

Given that digital wallets are provided free of charge to individuals, one economic value for private organisations to participate in the wallet ecosystem lies in business adoption of wallets. Other values are the time gains of using business wallets for automated transactions and security gains by being able to authenticate and validate other parties with the help of trust anchors. Since the wallet ecosystem increases its value by increasing the number of participants involved, the involvement of the private sector is important to achieving a critical mass in the rollout and use of wallets. This is particularly relevant in countries like Sweden, where well-established digital identification solutions for individuals such as BankID already offer secure and user-friendly services. For a European wallet to gain traction in such contexts, it must offer clear added value – such as for the user to save time in processes and clearly noticeable enhanced security or improved user experience as to encourage daily use – in order to encourage wallets as a complement to existing solutions.

While legislative frameworks such as eIDAS 2.0 provide the necessary legal foundation for digital wallets, the adoption of wallets should not be driven by legal obligations alone. Instead, **adoption must be grounded in clear value propositions**, **demonstrable efficiency gains**, and **tangible benefits to users and businesses alike**. For the technology to achieve its potential, participants must perceive real and immediate value beyond compliance requirements.

Feedback during the pilot revealed that businesses, in particular, currently see limited incentives to participate compared to individuals. The value proposition for businesses must be significantly strengthened, emphasizing not only the operational efficiencies but also strategic advantages such as faster market entry, reduced administrative costs, and improved data security.

A major overarching goal of the European wallet ecosystem is to strengthen the functional Single Market. However, this broader ambition often becomes diluted in practice, as the **concrete benefits for businesses are not always made explicit**. The focus on achieving a frictionless internal market must remain central in communications and service design to avoid losing sight of this key objective.

Another observation is that the technical sophistication behind digital credentials is often invisible to users. While users can easily grasp practical benefits like reduced paperwork and faster processes (aligning with the "once-only" principle), the underlying "smartness" of the credentials – the ability to selectively disclose, the trust frameworks, and the security mechanisms – often goes unrecognized. This highlights the need for better user education and simpler messaging.

Going forward, it is strongly advised that future Large-Scale Pilots place greater emphasis on adoption strategies. Adoption cannot be an afterthought; it must be a core pillar of design, development, and deployment activities. This includes involving end-users early, demonstrating value in concrete terms, and ensuring that adoption metrics are tracked and optimized throughout the project lifecycle.

4. The importance of the EUID as organisational identifier in the LPID

The business registries are the authoritative source for the LPID, and it can be assumed that they will, in some countries, also act as LPID issuers. All business registries already have the EUID registered, as its use is mandatory under EU projects and directives such as BRIS, BORIS, and the Company Law Directive (2017/1132). It is also a reasonable assumption that the LPID will need to be issued at a LoA high, which would likely require real-time verification of representatives and other security measures directly linked to processes and data within authentic sources.

If business registries were required to issue an organisational identifier under the control of third parties – such as the DUNS, LEI, or similar identifiers – they would not be able to guarantee the integrity of the organisational ID and thus the issuance process. Furthermore, relying on third party controlled organisational identifiers would introduce unnecessary and complex dependencies for revocation procedures.

Additionally, business registries would have to pay for these identifiers, as this data is not provided free of charge – unlike the EUID.

The technical structure of the EUID can be applied to all types of legal persons, including those not yet covered by the Company Law Directive. The EUID is already implemented by businesses.

4.7.5 Recommendations

A. Technical recommendations

- Map out a process for Legal person wallets of how a lost wallet should be handled.
- Consider format agnostic attestation presentation definitions, instead of format dependent presentation definitions.
- Drive the development of free open-source software (FOSS) SDKs for attestation handling (ideally also for the OpenID4VC protocol).
- Address schema evolution, and its impact on existing, issued attestations.
- Define recommendations on how to supplement EU wide attestations with additional, national level information.

- Further investigate reissuance both from a technical and business standpoint, and reissuance mechanisms and their reliability with longer periods without internet connectivity.
- Pilot a machine-to-machine use case for legal person wallets to ensure that the protocols and standards in the ARF fully support the legal person wallets use cases.
- Further define business rules around the standard attestations, such as revocation mechanisms, expiry and rules of reissuing.

B. Legal recommendations

- Taking into account the way EWC defined LPID and the consideration that EUID will be the best ID to use with the LPID, regulation between company law, beneficial ownership and Digital Identity Wallet/European Business Wallet should be harmonised.
- Work should be done on whether EUID can be further extended to entities in public sector and sole traders operating under organizational ID and other entities not covered by the Company Law Directive.
- Provide more clarity on the upcoming legislation on European Business Wallet.
- Further work on trust framework and clarify LoA High requirements and how these are met when re-issuance of LPIDs is proposed without user action.
- Analyse which representatives are authorized to apply for and sign the application for an LPID, which organizational statuses qualify for LPID issuance, and which attestations should be provided in a format compatible with EUDIWs.
- Analyse which laws need to be adapted on a national level to be able to issue attestations (including LPID) fully digitally.
- Further exploration is needed to determine how and whether the same integrity and data protection requirements, such as pseudonyms, anonymity, data minimization, selective disclosure, and collusion tracking, apply to organizational data and use cases.

C. Business recommendations

- **Active participation in European fora and pilots:** National business registries should actively participate in EU forums and pilot projects where the Digital Identity Wallet is being discussed and developed. This includes contributing to EU Commission expert groups and engaging in Large Scale Pilots related to organizational identities, such as the "We Build" project. Appointing dedicated subject-matter experts to follow pilot progress, provide national use cases, and share experiences in international workshops will be essential.
- **Initiating national pilots for Business Wallets:** Business registries should take the lead in launching national pilot projects to test the issuance of digital credentials, such as digital company certificates, in a wallet environment. Practical Proof-of-Concept initiatives with selected national companies will provide valuable insights and strengthen registries' positions as pioneers.
- **Developing electronic attribute attestation services:** Registries must quickly lay the groundwork to become qualified attribute issuers under the new eIDAS 2.0 rules. This involves meeting strict security and organizational requirements and creating APIs and backend systems to issue structured data in verifiable credential formats. Cooperation with national supervisory authorities will be crucial to obtain formal accreditation as a trusted provider.
- **Ensuring technical compatibility with EU frameworks:** Business registries must align their technical systems with the EU's Architecture and Reference Framework

(ARF) and other interoperability standards. IT architects should participate in international standardization efforts, and registries must ensure that their digital credentials (e.g., organizational numbers, EUIDs) are machine-readable and interoperable across borders.

- **Influencing policy and standards through consultations:** Registries should proactively contribute to European consultations and workshops related to the Digital Identity Wallet. National interests—such as the inclusion of organizational numbers and EUIDs as standard attributes—must be safeguarded. Close collaboration with ministries and Nordic peers can amplify influence.
- **Cooperating with private wallet providers:** Where private actors are selected to deliver wallet applications, business registries must engage early to ensure that organizational wallet functionalities are properly included. Partnerships can also help define user-friendly flows and integration points for business use cases.
- **Investing in information and capacity building:** Internally, registries must increase their organizational competence on EU frameworks, digital identity, and emerging wallet technologies. Externally, they should inform and prepare businesses for the upcoming changes through webinars, white papers, and direct stakeholder engagement. Building a national ecosystem that understands and embraces the Business Wallet concept will be key to successful adoption.

4.8 P4.4.1 Company authorized business travel and eInvoicing

4.8.1 Assessment summary

The following tables provide an overall assessment of the pilot. The first table evaluates the pilot's performance against its own defined goals, while the second assesses the extent to which the pilot achieved its intended ambition level.

Table 24 P4.4.1 own goals evaluation table

Goal Description	Rate (1-5)*	Comments
Demonstrate digital authorization	4	The pilot successfully showcased the use of verifiable Power of Attorney (PoA) attestation issued by the company, confirming that the employee was authorized to make bookings. However, the PoA scheme used is not yet standardized
Enable seamless booking experience	4	The integration of the EUDIW enabled the automatic verification of the employee and company identities reducing manual steps. However, some variations in wallet invocation methods (e.g, QR vs eAddress) create minor inconsistencies that could be further improved in future iterations
Reduce cost and time	4	The pilot showed clear potential to save time and reduce overhead for both employees and companies.
Automate post transaction invoicing	5	The pilot achieved automated invoicing via Peppol using structured LPID data to look up the company's Peppol Id and send the invoice directly. No manual intervention was required by the employee, fully demonstrating the value of verifiable company attestations.

***(Rates from 1 = not achieved to 5= fully achieved or N/A = Not Applicable, Not Available)**

Table 25 P4.4.1 evaluation on ambition level achievement

KPI	Target planned within pilot	Achieved	Please specify names of the achieved KPIs	Comment: if your commitment differs from the initially planned (D3.5), explain why
Number of wallet issuing countries	2	2	Finland, Norway	
Number of ODI issuing countries	2	2	Finland, Norway	
QEAA (PubEAAs)	4	4	NPID, LPID, EUCC, PoA	
Number of relying parties	1	1	Stellar Travel Agency	
QTSP providers	0	-	Out of scope	
Wallet users (legal persons)	2	2	Norwegian company using iGrant Enterprise Wallet solution. Finnish company using Mini-Wallet	
Wallet users (natural persons)	1	2	Finnish and Norwegian Employees using individual wallet (iGrant or Validated ID)	
Number of transactions completed	4	8	Presentation of Finnish NPID, LPID, EUCC, PoA Presentation of Norwegian NPID, LPID, EUCC, PoA	
Number of qualified signatures issued	0	-	Out of scope	
Number of ODI credentials shared	2	2	LPID, EUCC	

4.8.2 Pilot execution in production environment

A new prototype Travel Agency system was built for the pilot. In parallel, a Verifier component was also implemented to enable the validation of verifiable attestations. This component acts as a wrapper for OID4VP based presentation and verification functionalities, designed for easy integration with the Travel Agency system. It is built with re-usability in mind allowing the same component to be deployed across multiple pilots (such as the “Automated verification of Economic Operator identity in public procurement” pilot) and can be extended in future projects involving verifiable attestations

Co-funded by
the European Union

Table 26 P4.4.1 execution context

Name of the system	Production	Pre-production /acceptance	Clone of production built for the pilot	New prototype built for the pilot
Stellar Travel Agency				X
Verifier				X

The transactions performed were the presentation of EUCC and LPIDs for Norwegian and Finnish companies, along with NPIDs and PoAs of their respective employees. All data used in the pilot were test data and did not represent real companies of natural persons.

4.8.3 Pilot user testing feedback

Due to limited time and focusing more on the cross-border interoperability dimension (implementation of two iterations) and conformance testing with the EWC test best, no formal user testing with structured user testing questionnaire was conducted. Testing was limited to engaging test users that were aware of the process of booking a business trip and invoicing it to the company. The test users went through the whole process in both iterations and commented that:

- The wallet enabled ecosystem allowed for much faster booking process than traditional methods. There is no need to manually enter company details and forward approval emails.
- Presenting the PoA was simple and there was no need to chase down trails of email threads for approval.
- No need for claiming expenses. The users valued the invoicing automation.
- The wallet interactions felt fragmented. Some credentials were presented by scanning QR codes while others used other methods of wallet invocation. It would be smoother if the presentation was consistent.
- It can potentially simplify business travel overhead for companies. Less overhead, fewer mistakes and easier to track expenses.

4.8.4 Insights and lessons learnt

PoA Schema not available

At the time of the pilot's technical implementation, there is no EWC agreed schema definition for the PoA available in the EWC public repositories. The PoA data scheme is crafted to cover the pilot's needs but may conflict with the EWC published PoA data scheme whenever it becomes available or the one that will be developed in WE BUILD.

Interoperability issues

Interoperability issues arise between wallet implementations, Issuers, and Relying Parties. For example, some wallets may only support a specific client_id_scheme, requiring Relying Party to accommodate for multiple-schemes and all the different OID4VP presentation request fields for each scheme. Additionally, there is no guarantee of backwards compatibility. If a wallet implementation upgrades to OID4VP draft 21, while the Relying Party still uses OID4VP draft 18 the interaction may break due to incompatibilities between versions.

Lack of technical readiness and technical examples

Many issuers are not yet technically prepared to issue verifiable attestations (VCs). The technical flows can be complex, especially for those without prior experience with OID4VC. Providing a test EWC reference issuer and verifier would help developers better understand and experiment with the complete OID4VCI and OID4VP flows, facilitating learning and adoption.

Security concerns

There is no high LoA available, and the trust framework is not implemented yet. Security concerns will arise when it comes to real-world transactions.

Lack of standardization of wallet invocation mechanisms

There is no standardization for wallet invocation mechanisms, which introduced integration complexity between implementation phases. During the initial phase of the pilot, the Finnish wallet (Mini-Wallet) supported invocation using eAddress based requests. However, in the later phase involving the Norwegian use case, the Enterprise wallet solution (iGrant) did not support invocation through eAddress presentation requests. This required further changes and added technical overhead.

4.8.5 Recommendations

- Further work is needed on PoA data model and data scheme.
- Align on standardizing invocation protocols/mechanisms and adopt a consistent approach that will enhance interoperability across wallet providers and Relying Parties, especially in cross-border scenarios.
- Have stable and mature specifications, as interop testing gets very challenging with different versions of specifications.
- Provide a test reference issuer and verifier which would help developers to better understand and experiment with the complete OID4VCI and OID4VP flows, facilitating learning and adoption.
- Implement a trust framework that can be used in order to scale to deployment and production transactions.

5. Conclusions

5.1 Final pilot results

Table 27 presents the final state of business scenario pilot implementations.

Table 27 Final pilot results

Business Scenario Pilots	Status
P1.1.1 - Issue and verify attestations for evidence in the procurement process (ESPD)	Technical readiness achieved
P1.1.2 - Automated verification of Economic Operator identity and mandate in the ESPD	Technical readiness achieved
P2.1.1 - Onboarding new business partner	Technical readiness achieved
P2.2.1 - Open a bank account for a business	Technical readiness achieved
P 3.1.1 - Domain holder verification by domain registry	Did not proceed to implementation as strategic partners (SIDN) left the project
P3.2.1 - Domain ownership as credential for QWAC issuance	Did not proceed to implementation due to reduced interest
P4.1.1 - Peppol network registration and use	Technical readiness achieved
P4.2.1 - Verifiable eReceipt	Technical readiness achieved
P4.3.1 - Create a company branch in another country	Technical readiness achieved
P4.4.1 - Company authorised business travel and eInvoicing	Technical readiness achieved

Eight (7) out of **nine (9) pilots** originally committed to by the beneficiaries in D3.5 have achieved technical readiness (green colour) which signifies the completion of technical work. Since the writing of D3.5, **one (1) additional pilot** called “Company Authorized Business Travel and eInvoicing” was implemented and achieved technical readiness.

The pilots from BA3 “Domain registration: did not materialize (P3.1.1 Domain holder verification by domain registry and P3.2.1 Domain ownership as credential for QWAC issuance) due to the fact that SIDN who was the business area owner left the project and although there was an attempt to make it happen, finally these pilots did not proceed to implementation.

5.2 Summary of attestations and wallets used

Table 28 presents a summary of EUDI wallets and attestations used in each pilot.

Table 28 Summary of attestations and wallets used

Business Scenario Pilots	Business Wallet	Personal Wallet	Attestations
P1.1.1 - Issue and verify attestations for evidence in the procurement process (ESPD)	iGrant.io Organization Wallet	iGrant.io Data Wallet	LPID
P1.1.2 - Automated verification of Economic Operator identity and mandate in the ESPD	1st iter.: Mini-Wallet 2nd iter.: iGrant Organization Wallet	iGrant.io Data Wallet	LPID, EUCC, NPID
P2.1.1 - Onboarding new business partner	Archipels Business	Archipels wallet	LPID, NPID, EUCC, IBAN, UBO, Signatory Rights, KBIS
P2.2.1 - Open a bank account for a business	1st iter.: Bosch 2nd iter.: Mini-Wallet 3rd iter.: Mini-Wallet	1st iter.: iGrant.io Data wallet 2nd iter.: Lissi 3rd iter.: Mini-Wallet	NPID, LPID, EUCC, PoA
P4.1.1 - Peppol network registration and use	Archipels Business	Archipels wallet	LPID, KBIS
P4.2.1 - Verifiable eReceipt	iGrant.io Organization Wallet	Lissi, Validated ID, iGrant.io Data wallet	vReceipt
P4.3.1 - Create a company branch in another country	iGrant.io Organization Wallet	iGrant.io Data wallet	EUCC, NPID, LPID
P4.4.1 - Company authorised business travel and eInvoicing	1st iter.: Mini-Wallet 2nd iter.: iGrant Organisational Wallet	iGrant Data Wallet	LPID, NPID, EUCC, PoA

5.3 Concluding remarks and recommendations

The implementation and evaluation of the **eight business scenario pilots** conducted within WP3 of EWC are a good starting way of demonstrating the real-world potential of the Legal person Wallet (European Business Wallet). These pilots have provided genuine contributions and concrete evidence to the understanding on how legal person wallets with LPID (PID for legal persons) and standardised attestations in a secure, and interoperable wallet ecosystem can significantly enhance trust, efficiency, and user experience in a wide range of domestic and cross-border business processes. Feedback from participating companies in the EWC pilots has clearly indicated the importance of enabling organisations to use wallets for their business transactions – whether with other companies, individuals, or public authorities – across the EU.

The business enabled wallet ecosystem can reduce administrative burdens through the automation of data sharing and verification (e.g., in procurement and onboarding processes), improve data integrity and trust by enabling the use of verified, up-to-date credentials issued by authentic sources; accelerate cross-border interactions, particularly in scenarios such as public tenders, banking, and company branch registration, strengthen fraud prevention and compliance, especially in areas involving financial or regulatory oversight (e.g., KYC/AML and ESPD processes), and empower SMEs by lowering barriers in making business in the Single Market and beyond. The potential for the use of business wallets is huge and the business wallet can really be a game changer for wider adoption and uptake of the wallet ecosystem.

The pilots demonstrated clear benefits across usability, process efficiency, data quality, and trust. However, they also revealed critical ecosystem challenges regarding user experience, ecosystem maturity, interoperability, governance and legal clarity.

The main issues identified from the implementation of the EWC WP3 business scenarios pilots can be summarized as follows:

- Most of the Issuing Authorities (Business Registries and Tax authorities) lacked the technical readiness and in-house expertise to issue LPIDs and VCs.
- Most pilots rely on test data due to change resistance from the businesses and due also to legal unclarity.
- There are interoperability issues between digital wallets, issuers and relying parties due to different id schemes or different versions implemented in different parties. For example, some wallets may support one specific client_id_scheme and the relying

parties need to support them all. If a wallet implementation upgrades on using OID4VP 21 but the relying party or issuer is using OID4VP 18, the whole flow may stop working due to incompatibilities.

- Security concerns: Understanding the whole LPID issuance process from a security standpoint is complex.
- Production-readiness: While some pilots were able to run in close to production environments, most of them remained in test environments using test data.
- User and stakeholder feedback: Wallet technology is not yet very known to users. Real-world testing shown the importance of clear onboarding processes and improvement of UX.
- More piloting is needed in different domains (public procurement, eInvoicing, KYS/KYC) to focus on specific requirements and how these can be enabled in the wallet ecosystem, to test the use of business wallets in different scenarios to demonstrate the benefits of using business wallets in the whole public procurement cycle. This includes piloting a machine-to-machine use case for legal person wallets to ensure that the protocols and standards in the ARF fully support the legal person wallets use cases.

We should also stress here that semantics and attestations is an area of work that needs more attention and close cooperation with different DGs is necessary (especially with DG JUST).

Harmonisation of regulations between company law, beneficial ownership and Digital Identity Wallet/European Business Wallet is important, if EUID will be finally decided to be the common company ID to use with the LPID.

The sustainability of the use of business wallets in eProcurement will depend on the alignment of the strategy between DG CONNECT, DG GROW and DG DIGIT regarding the compatibility of business wallet with the architecture of the Once Only Technical System (OOTS), as well as whether public procurement will use the OOTS at all.

Recommendations for scaling the business wallet in the different piloting domains:

- **Adoption strategies and education of involved stakeholders**
    - Develop adoption strategies for disseminating the value and benefits of business wallets and how companies using business wallets can do business simply and digitally.
    - Educate and explain to the users in plain language the concepts of wallets and attestations and how the business wallet comes to complement functionalities of the natural person wallet in the business processes and transactions.
    - Focus on targeted user awareness and engagement strategies, including onboarding early adopters to create an initial user base willing to pilot and further refine the solution.
    - Registries to inform and prepare businesses for the upcoming changes through webinars, white papers, and direct stakeholder engagement. Building a national ecosystem that understands and embraces the Business Wallet concept will be key to successful adoption.
- **Technical and interoperability recommendations**
    - Work further on the definition of the business wallet that EWC initiated, on legal binding and on protocol limitations and deficiencies across different wallets and multiple client id schemes.

  - Provide a test reference issuer and verifier which would help developers to better understand and experiment with the complete OID4VCI and OID4VP flows, facilitating learning and adoption.
  - Align on standardizing invocation protocols/mechanisms and adopt a consistent approach that will enhance interoperability across wallet providers and Relying Parties, especially in cross-border scenarios.
- **Semantics and attestations**
  - Work on the standardisation of LPID and EUCC schemas.
  - Further work on the PoA model definition and scope, and on the requirements for PoA issuers and pilot PoA in different business scenarios.
  - Work further on standardised, harmonized domain-specific rulebooks and data models addressing the consistent needs of (Q)EAAs, QTSPs, and relying parties across different European jurisdictions in order to support diverse use cases and global operators.
  - Define recommendations on how to supplement EU wide attestations with additional, national level information.
  - Introduce in the Implementing Acts on specifications and procedures for the catalogue of attributes a unified mechanism for the maintenance and sharing of schema versions.
  - Address schema evolution, and its impact on existing, issued attestations.
  - Further define business rules around the standard attestations, such as revocation mechanisms, expiry and rules of reissuing.
  - Consider format agnostic attestation presentation definitions, instead of format dependent presentation definitions.
- **Trust framework**
  - Implement a trust framework that can be used in order to scale to deployment and production transactions.
  - Work on the process for issuing (Q)EAA for legal persons and develop good practices that cover the specific needs of legal persons.
- **UX/UI**
  - Do more work on UX/UI in order to facilitate wallet adoption. Easy to follow guides with each step the users need to take for requesting and presenting attestations.
- **Alignment with other European initiatives**
  - Coordinate efforts by domain-specific expert groups to align legal and administrative requirements, e.g. align with public procurement and Once Only Technical System (OOTS).
- **Legal recommendations**
  - EWC considers that EUID is the best ID to use with the LPID, but this needs that regulation between company law, beneficial ownership and Digital Identity Wallet/European Business Wallet should be harmonised.
  - Work should be done on whether EUID can be further extended to entities in public sector and sole traders operating under organizational ID and other entities not covered by the Company Law Directive.
  - Provide more clarity on the upcoming legislation on European Business Wallet.
  - Further work on trust framework and clarify LoA High requirements and how these are met when re-issuance of LPIDs is proposed without user action.
  - Analyse which representatives are authorized to apply for and sign the application for an LPID, which organizational statuses qualify for LPID

    issuance, and which attestations should be provided in a format compatible with EUDIWs.
  - Analyse which laws need to be adapted on a national level to be able to issue attestations (including LPID) fully digitally.
  - Further exploration is needed to determine how and whether the same integrity and data protection requirements, such as pseudonyms, anonymity, data minimization, selective disclosure, and collusion tracking, apply to organizational data and use cases.
- **Initiating national pilots for Business Wallets**
  - Business registries should take the lead in launching national pilot projects to test the issuance of digital credentials, such as digital company certificates, in a wallet environment. Practical Proof-of-Concept initiatives with selected national companies will provide valuable insights and strengthen registries' positions as pioneers.
- **Developing electronic attribute attestation services**
  - Registries must quickly lay the groundwork to become qualified attribute issuers under the new eIDAS 2.0 rules. This involves meeting strict security and organizational requirements and creating APIs and backend systems to issue structured data in verifiable credential formats. Cooperation with national supervisory authorities will be crucial to obtain formal accreditation as a trusted provider.

Eight business scenario pilots in total were implemented and achieved technical readiness and provided valuable feedback. Seven of them were defined in deliverable D3.5 and a new pilot regarding company authorized business travel and eInvoicing was added later.

The pilot evaluations presented in the deliverable demonstrate a promising potential of the EUDIW. Despite ongoing challenges, such as standardization, production deployment and user onboarding, the pilots have successfully laid the foundation for broader adoption, policy alignment and further exploring the utilization of EUDIW across European organizations. They demonstrate not just the technical feasibility but the transformative potential of the business wallet. They offer a vision of a more secure, efficient, and inclusive European digital economy – where businesses, especially SMEs, can seamlessly operate across borders. To realize this vision, further work is needed to transition from pilot to production, and this will continue in the new Large Scale Pilot project WE BUILD which kicks-off in September 2025.

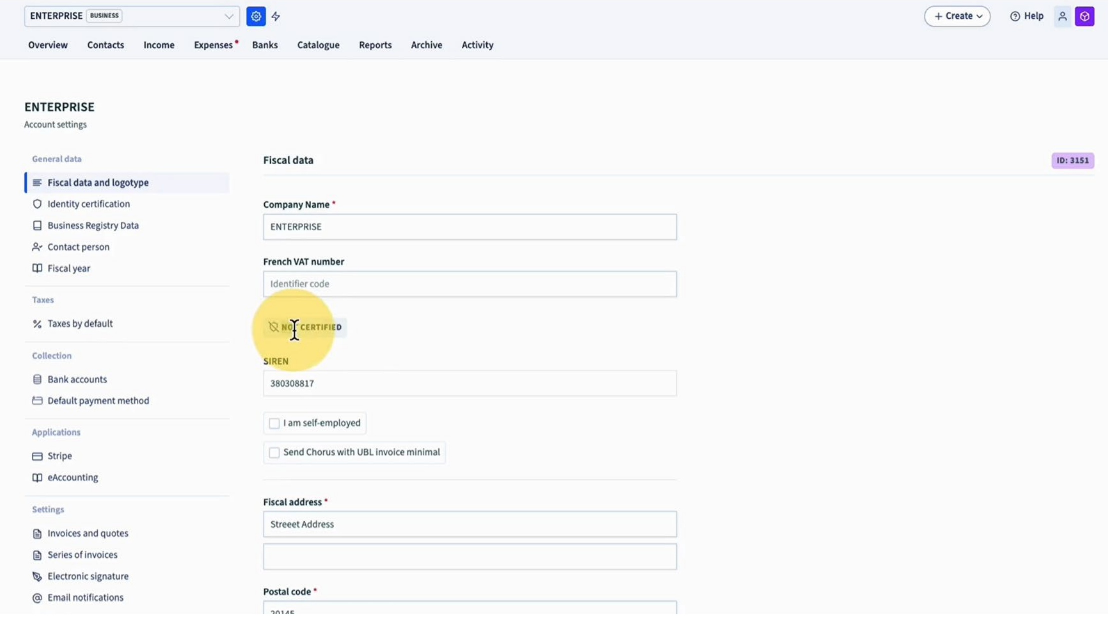
Annex A: User Journey Screenshots

Company Verification process – B2BRouter Verifier

The following section shows the implemented pilot solution process illustrated using screenshots:

1. **A company/user (holder) registers on B2Brouter (verifier) and settles username and password.**

Figure 25 shows that the user does not have a ceritified and approved account yet. The user has entered a SIREN number that is associated to the account but that is not verifier yet.



ENTERPRISE BUSINESS

Overview Contacts Income Expenses Banks Catalogue Reports Archive Activity

+ Create Help

ENTERPRISE
Account settings

General data
- Fiscal data and logotype
- Identity certification
- Business Registry Data
- Contact person
- Fiscal year

Taxes
- Taxes by default

Collection
- Bank accounts
- Default payment method

Applications
- Stripe
- eAccounting

Settings
- Invoices and quotes
- Series of invoices
- Electronic signature
- Email notifications

Fiscal data ID: 3151

Company Name *
ENTERPRISE

French VAT number
Identifier code

NOT CERTIFIED

SIREN
380308817

□ I am self-employed

□ Send Chorus with UBL invoice minimal

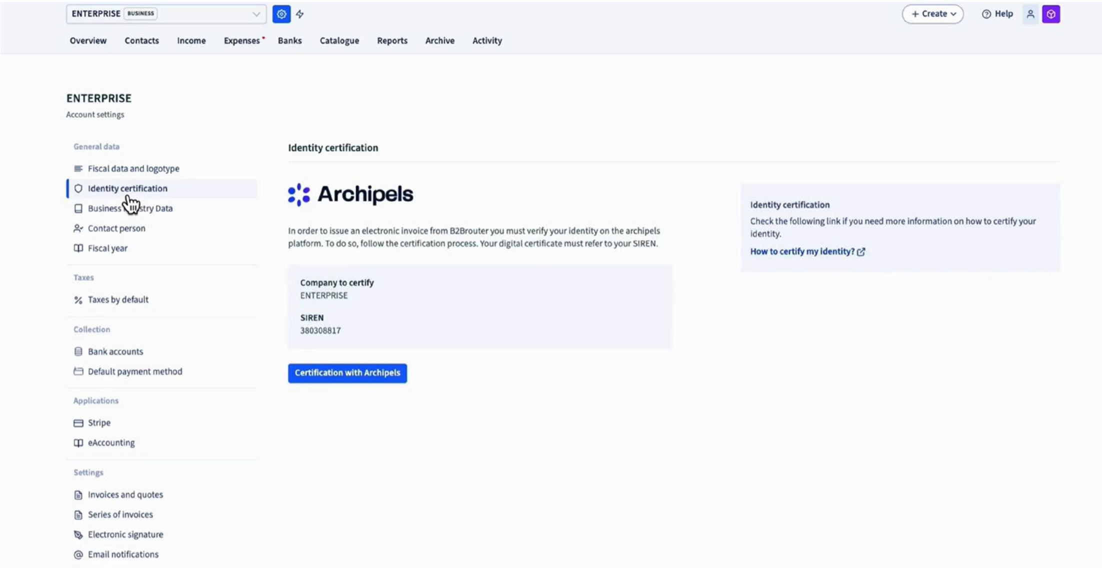
Fiscal address *
Streeet Address

Postal code *
20145

Figure 25 Company registration

2.The B2Brouter platform (verifier) then asks the End-user to present its KBIS attestation to verify its account data.

The user therefore accesses the Identity Certification menu (Figure 26) which lets him verify his identity about the Archipels platform. The digital certificate must relate to the SIREN number entered into the B2Brouter platform



ENTERPRISE BUSINESS

Overview Contacts Income Expenses Banks Catalogue Reports Archive Activity

+ Create Help

ENTERPRISE
Account settings

General data
- Fiscal data and logotype
- Identity certification
- Business Registry Data
- Contact person
- Fiscal year

Taxes
- Taxes by default

Collection
- Bank accounts
- Default payment method

Applications
- Stripe
- eAccounting

Settings
- Invoices and quotes
- Series of invoices
- Electronic signature
- Email notifications

Identity certification

Archipels

In order to issue an electronic invoice from B2Brouter you must verify your identity on the archipels platform. To do so, follow the certification process. Your digital certificate must refer to your SIREN.

Company to certify
ENTERPRISE

SIREN
380308817

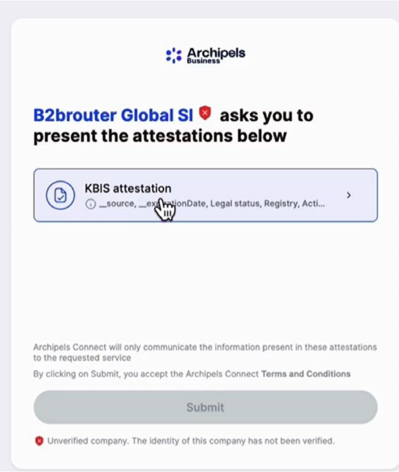
Certification with Archipels

Identity certification
Check the following link if you need more information on how to certify your identity.
How to certify my identity?

Figure 26 Identity certification menu

3.The company/user (holder) authenticates with EUDI Wallet solution of Archipels (EUDI Wallet Provider).

a) The user is forwarded to the Archipels platform and asked to present the KBIS attestation to B2Brouter Figure 27.



Archipels Business

B2brouter Global SI asks you to present the attestations below

KBIS attestation
__source, __expirationDate, Legal status, Registry, Acti...

Archipels Connect will only communicate the information present in these attestations to the requested service

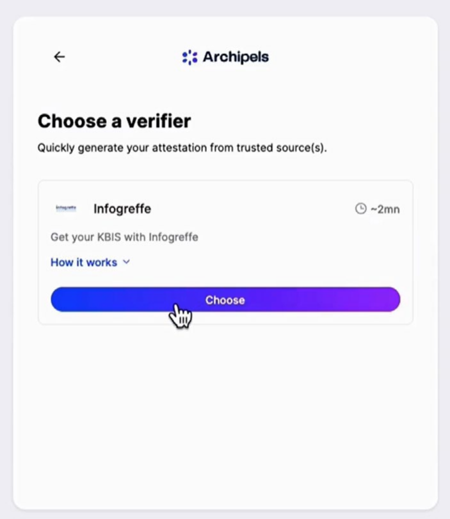
By clicking on Submit, you accept the Archipels Connect **Terms and Conditions**

Submit

Unverified company. The identity of this company has not been verified.

Figure 27 KBIS attestation

b) Infogreffe is chosen as (Q)EAA provider to generate the corresponding KBIS attestation form trusted source (Figure 28).



Archipels

Choose a verifier

Quickly generate your attestation from trusted source(s).

Infogreffe ~2mn

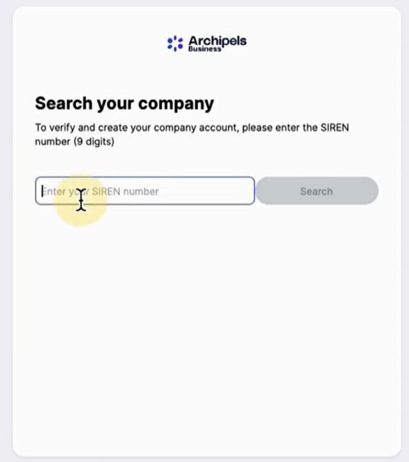
Get your KBIS with Infogreffe

How it works

Choose

Figure 28 (Q)EAA provider selection

c) The user needs to enter his SIREN Number to verify the company account Figure 29



Archipels Business

Search your company

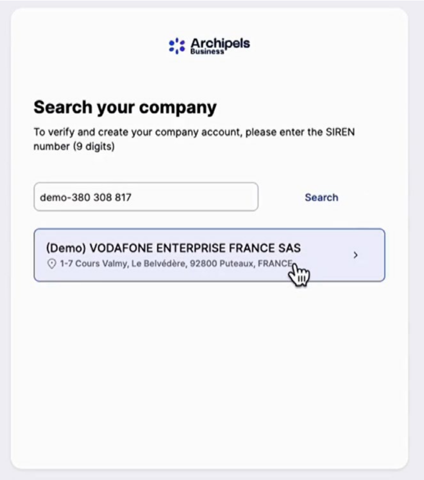
To verify and create your company account, please enter the SIREN number (9 digits)

Enter your SIREN number

Search

Figure 29 Company account verification

d) The company associated to the SIREN number is shown and must be selected by the user (Figure 30)



Archipels Business

Search your company

To verify and create your company account, please enter the SIREN number (9 digits)

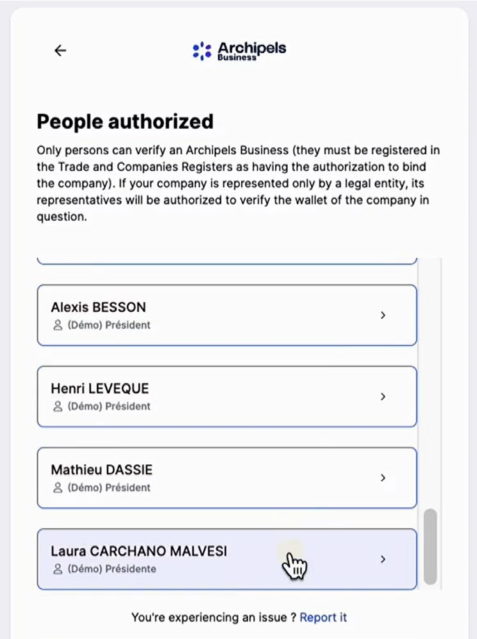
demo-380 308 817

Search

(Demo) VODAFONE ENTERPRISE FRANCE SAS
1-7 Cours Valmy, Le Belvédère, 92800 Puteaux, FRANCE

Figure 30 Company selection

e) The user that is doing the verification for the company must select an authorized person that is connected to the company in the Trade and Company register. Only authorized person acting on behalf of the user (company) can execute the verification process (Figure 31)



Archipels Business

People authorized

Only persons can verify an Archipels Business (they must be registered in the Trade and Companies Registers as having the authorization to bind the company). If your company is represented only by a legal entity, its representatives will be authorized to verify the wallet of the company in question.

Alexis BESSON
(Démo) Président

Henri LEVEQUE
(Démo) Président

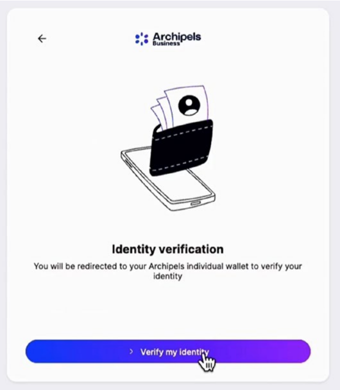
Mathieu DASSIE
(Démo) Président

Laura CARCHANO MALVESI
(Démo) Présidente

You're experiencing an issue ? Report it

Figure 31 Selection of authorized person

f) The authorized person acting on behalf of the user (company) must verify their identity on the Archipels platform (Figure 32)

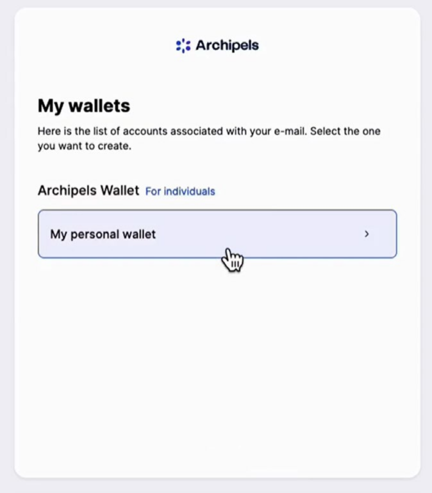


Identity verification

You will be redirected to your Archipels individual wallet to verify your identity

Figure 32 Identity verification

g) The authorized person acting on behalf of the user (company) must select the appropriate person wallet connected to his account (Figure 33)



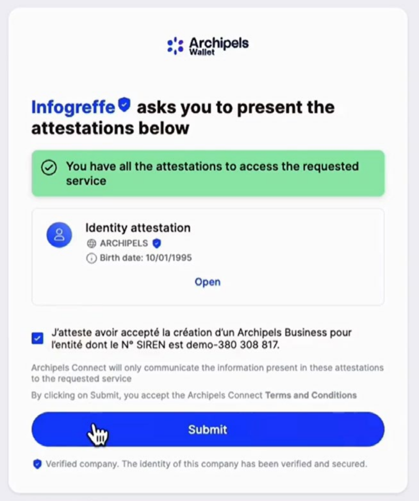
My wallets

Here is the list of accounts associated with your e-mail. Select the one you want to create.

Archipels Wallet For individuals

Figure 33 Personal wallet selection

h) The (Q)EAA provider Infogreffe asks the authorized person acting on behalf of the user (company) to present an Identity Attestation (Figure 34)



Infogreffe asks you to present the attestations below

You have all the attestations to access the requested service

Identity attestation
ARCHIPELS
Birth date: 10/01/1995

☑ J'atteste avoir accepté la création d'un Archipels Business pour l'entité dont le N° SIREN est demo-380 308 817.

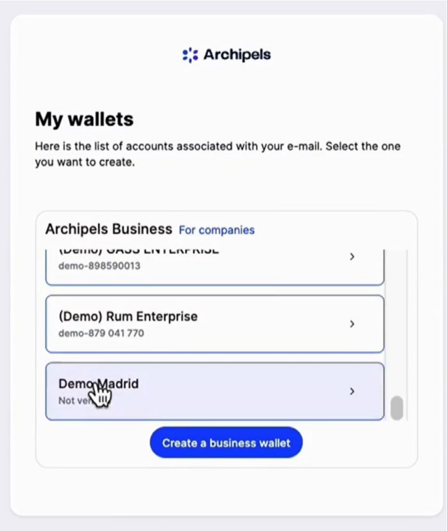
Archipels Connect will only communicate the information present in these attestations to the requested service

By clicking on Submit, you accept the Archipels Connect **Terms and Conditions**

Verified company. The identity of this company has been verified and secured.

Figure 34 Identity presentation

i) The user or authorized person must select the appropriate Organization Wallet (Figure 35)



Archipels

My wallets

Here is the list of accounts associated with your e-mail. Select the one you want to create.

Archipels Business For companies

(Demo) GASS ENTERPRISE
demo-898590013

(Demo) Rum Enterprise
demo-879 041 770

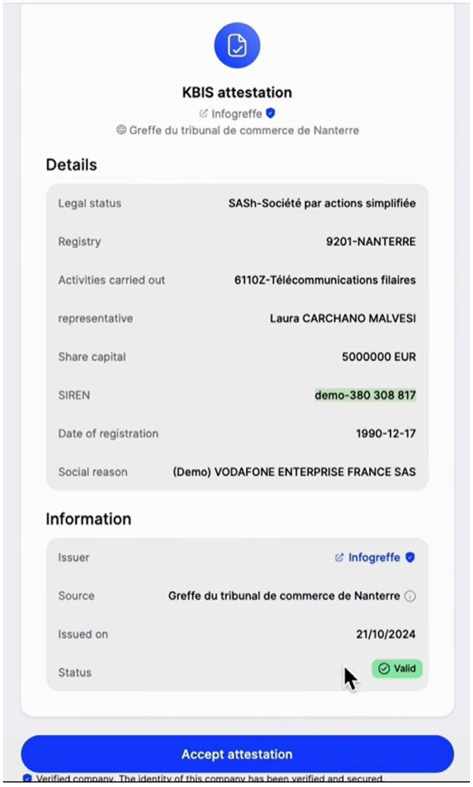
Demo Madrid
Not ve

Create a business wallet

Figure 35 Organizational Wallet selection

4.Infogreffe, being the (Q)EEA Issuer (service) delivers the KBIS attestation to the holder, for approval using Archipels EUDI Wallet solution as QTSP

a) The details of the KBIS attestation and especially the SIREN number associated with the organization are shown to the authorized person acting on behalf of the user (company) for acceptance (Figure 36)



KBIS attestation

Infogreffe

Greffe du tribunal de commerce de Nanterre

Details

Legal status	SASh-Société par actions simplifiée
Registry	9201-NANTERRE
Activities carried out	6110Z-Télécommunications filaires
representative	Laura CARCHANO MALVESI
Share capital	5000000 EUR
SIREN	demo-380 308 817
Date of registration	1990-12-17
Social reason	(Demo) VODAFONE ENTERPRISE FRANCE SAS

Information

Issuer	Infogreffe
Source	Greffe du tribunal de commerce de Nanterre
Issued on	21/10/2024
Status	Valid

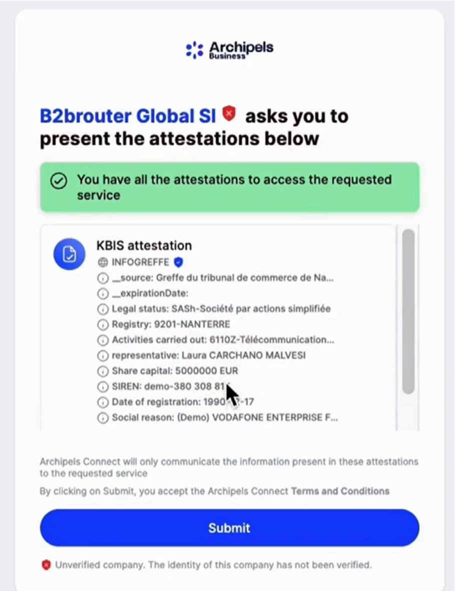
Accept attestation

Verified company. The identity of this company has been verified and secured.

Figure 36 Details of KBIS attestation

b) The authorized person acting on behalf of the user (company) is asked to present the attestation to B2Brouter. The authorized person can preview the data submitted to B2Brouter and can confirm the transmission (Figure 37)

Co-funded by the European Union



Archipels Business

B2brouter Global SI asks you to present the attestations below

You have all the attestations to access the requested service

KBIS attestation

INFOGREFFE

- __source: Greffe du tribunal de commerce de Na...
- __expirationDate:
- Legal status: SASh-Société par actions simplifiée
- Registry: 9201-NANTERRE
- Activities carried out: 6110Z-Télécommunication...
- representative: Laura CARCHANO MALVESI
- Share capital: 5000000 EUR
- SIREN: demo-380 308 81
- Date of registration: 1990 [illegible]-17
- Social reason: (Demo) VODAFONE ENTERPRISE F...

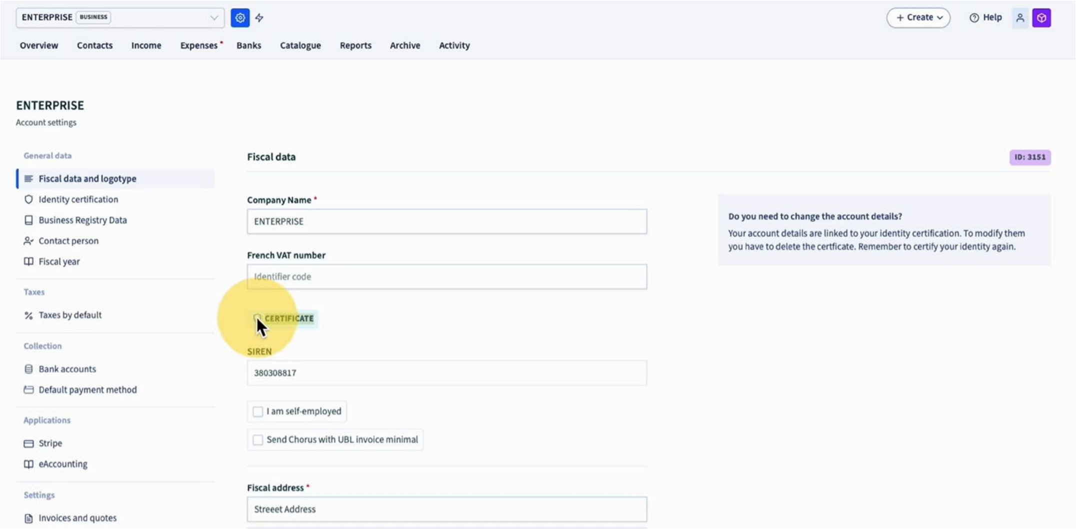
Archipels Connect will only communicate the information present in these attestations to the requested service

By clicking on Submit, you accept the Archipels Connect **Terms and Conditions**

Unverified company. The identity of this company has not been verified.

Figure 37 Data preview

5.B2Brouter (Verifier) verifies the company and authenticity of the KBIS attestation and recognizes the organization as a certified organization (Figure 38**)**



ENTERPRISE

Account settings

Fiscal data

ID: 3151

Company Name *: ENTERPRISE

French VAT number: Identifier code

CERTIFICATE

SIREN: 380308817

□ I am self-employed

□ Send Chorus with UBL invoice minimal

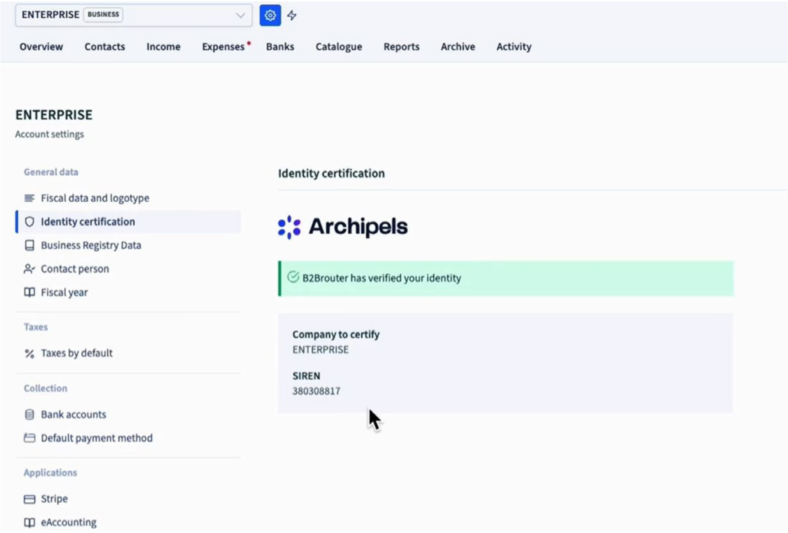
Fiscal address *: Streeet Address

Do you need to change the account details?

Your account details are linked to your identity certification. To modify them you have to delete the certficate. Remember to certify your identity again.

Figure 38 Company verification

The identity of the organization is verified (Figure 39)



B2Brouter has verified your identity

Company to certify
ENTERPRISE

SIREN
380308817

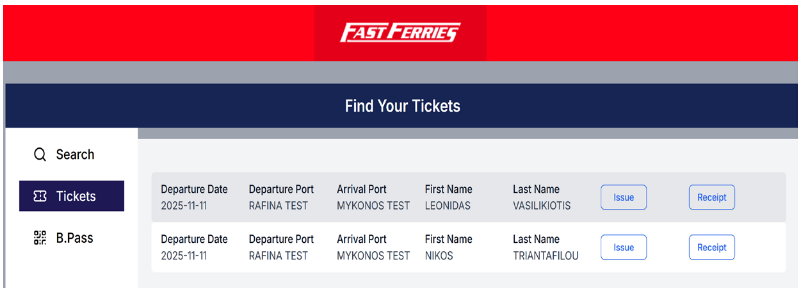
Figure 39 Company is verified

6.Seamless Access to Peppol and Other Services After Verification

After the certification and verification of company data, users can seamlessly access additional services like Peppol without requiring further verification. By agreeing to use their verified master data on B2Brouter, selecting an ID for Peppol registration, and accepting the Peppol Service Agreement, users gain immediate access to the Peppol network. Once these steps are completed, B2Brouter unlocks the Peppol service, enabling smooth and efficient electronic transactions. Also, these users/companies are marked as verified companies in the B2Brouter directory used to look up and verify trading partners.

Fast Ferries / Vero – vReceipt interfaces

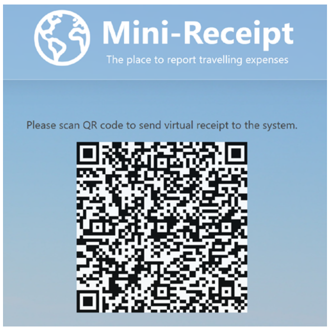
For phase 2 pilot, Fast Ferries / University of Aegean implemented a portal for usage scenario 1 where the user can download the (boarding pass and) vReceipt in their mobile wallet as showed in Figure 40.



Departure Date	Departure Port	Arrival Port	First Name	Last Name
2025-11-11	RAFINA TEST	MYKONOS TEST	LEONIDAS	VASILIKIOTIS
2025-11-11	RAFINA TEST	MYKONOS TEST	NIKOS	TRIANTAFILOU

Figure 40 Fast Ferries portal

The Finnish Tax Administration implemented a relying party to which the vReceipt can be presented, as showed in Figure 41 and Figure 42:

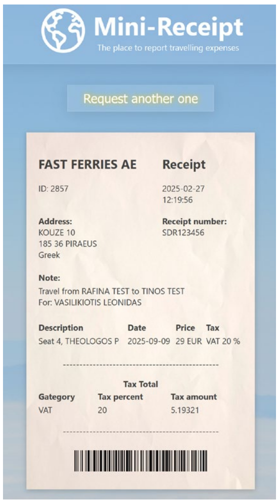


Mini-Receipt

The place to report travelling expenses

Please scan QR code to send virtual receipt to the system.

Figure 41 Presentation request vReceipt



Mini-Receipt

The place to report travelling expenses

FAST FERRIES AE **Receipt**

ID: 2857

2025-02-27
12:19:56

Address:
KOUZE 10
185 36 PIRAEUS
Greek

Receipt number:
SDR123456

Note:
Travel from RAFINA TEST to TINOS TEST
For: VASILIKIOTIS LEONIDAS

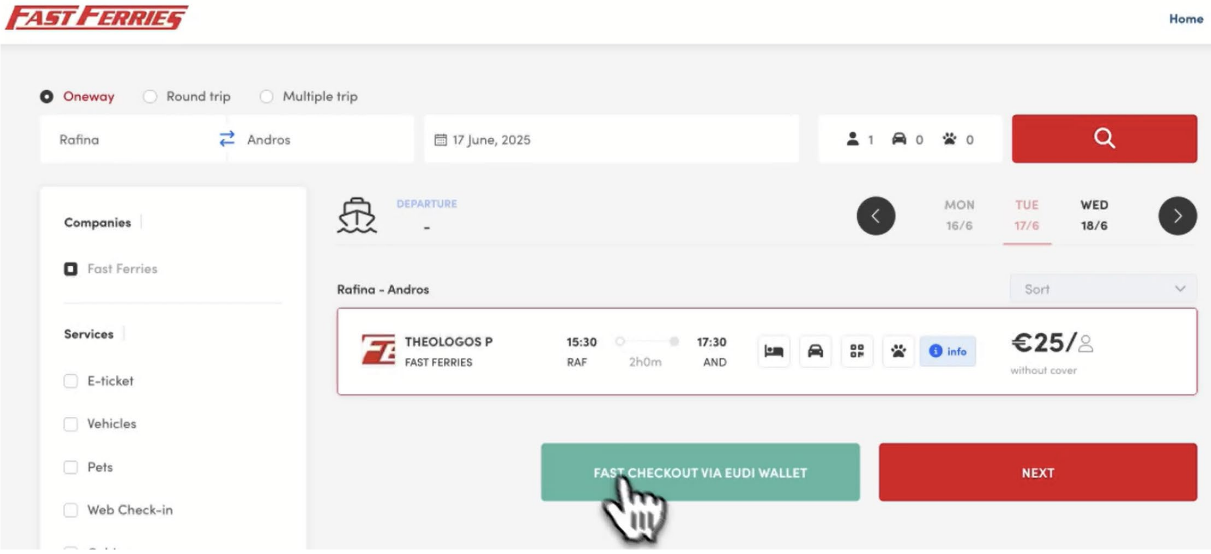
Description	Date	Price	Tax
Seat 4, THEOLOGOS P	2025-09-09	29 EUR	VAT 20 %

Tax Total

Gategory	Tax percent	Tax amount
VAT	20	5.19321

Figure 42 vReceipt visualised by Relying Party

For phase 3 pilot WP2/WP3 implemented the integrated flow described in RFC-011 where the payment with EUDIW and issuance of vReceipt is integrated in a single transaction (the service is available at https://wallet.fastferries.com.gr/). Figure 43- Figure 49 depict screenshots from the browser and phone UI describe the flow:



● Oneway ○ Round trip ○ Multiple trip

Rafina ⇄ Andros

17 June, 2025

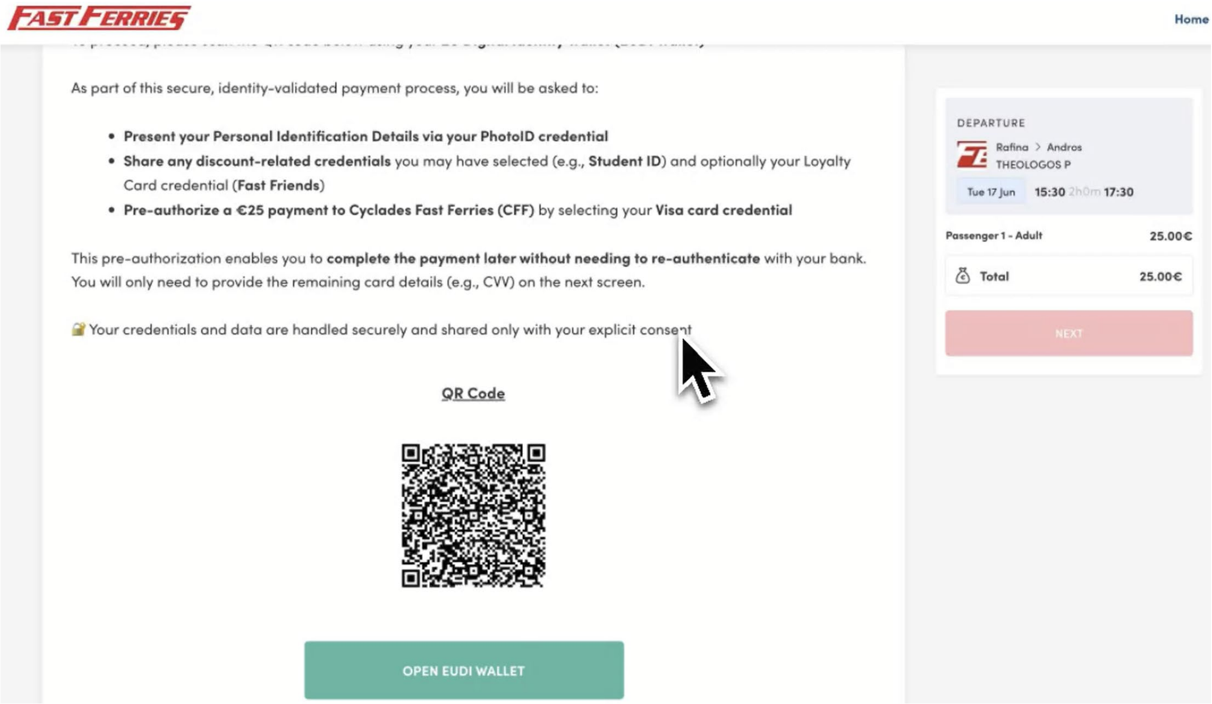
1 0 0

Rafina - Andros

THEOLOGOS P FAST FERRIES	15:30 RAF	2h0m	17:30 AND	info	€25/ without cover

Figure 43: 1. The user selects the ticket in the webshop and proceeds to checkout with EUDI wallet.

Co-funded by
the European Union



As part of this secure, identity-validated payment process, you will be asked to:

- **Present your Personal Identification Details via your PhotoID credential**
- **Share any discount-related credentials** you may have selected (e.g., **Student ID**) and optionally your Loyalty Card credential (**Fast Friends**)
- **Pre-authorize a €25 payment to Cyclades Fast Ferries (CFF)** by selecting your **Visa card credential**

This pre-authorization enables you to **complete the payment later without needing to re-authenticate** with your bank. You will only need to provide the remaining card details (e.g., CVV) on the next screen.

🔐 Your credentials and data are handled securely and shared only with your explicit consent

QR Code

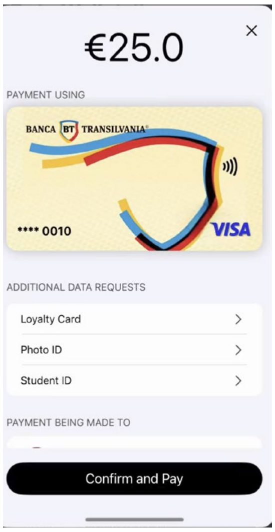
DEPARTURE

Rafina > Andros
THEOLOGOS P

Tue 17 Jun 15:30 2h0m 17:30

Passenger 1 - Adult	25.00€
Total	25.00€

Figure 44: 2. The webshop presents a QR code that the user scans with their wallet.



€25.0

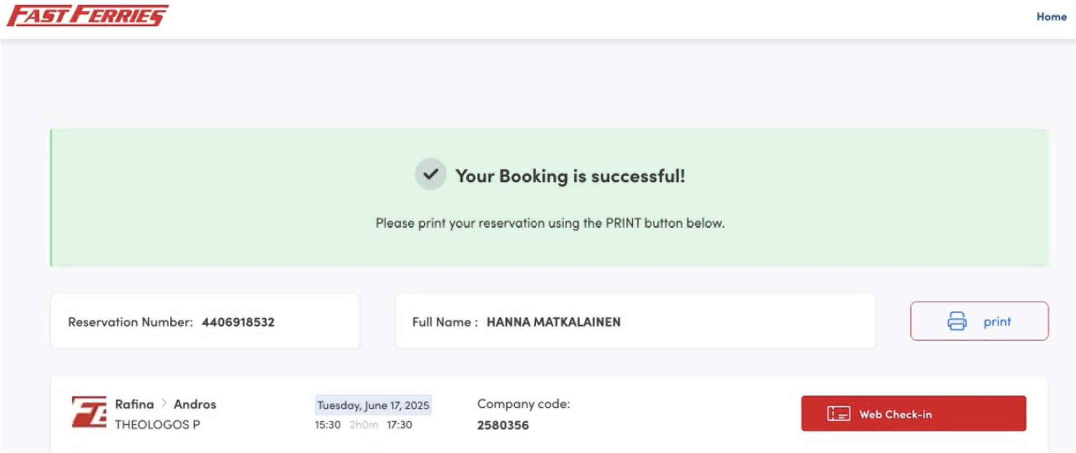
PAYMENT USING

ADDITIONAL DATA REQUESTS

- Loyalty Card
- Photo ID
- Student ID

PAYMENT BEING MADE TO

Figure 45: 3. The user authorizes the payment in their wallet.



Your Booking is successful!

Please print your reservation using the PRINT button below.

Reservation Number: 4406918532

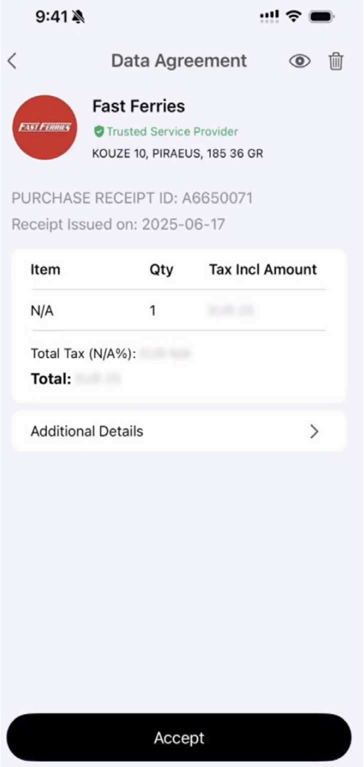
Full Name : HANNA MATKALAINEN

Rafina > Andros
THEOLOGOS P

Tuesday, June 17, 2025
15:30 2h0m 17:30

Company code:
2580356

Figure 46: 4. The webshop confirms the transaction is complete.



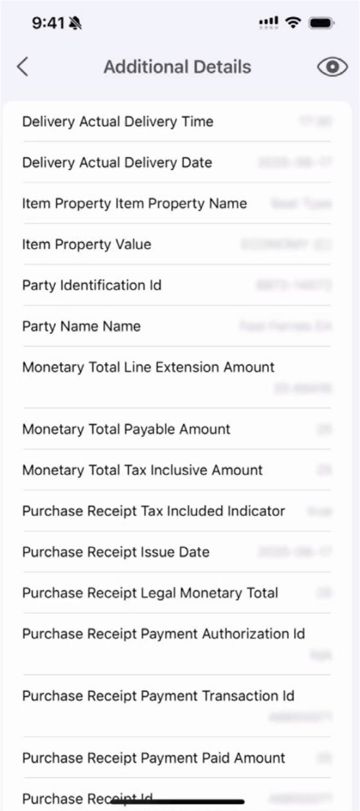
Fast Ferries
Trusted Service Provider
KOUZE 10, PIRAEUS, 185 36 GR

PURCHASE RECEIPT ID: A6650071
Receipt Issued on: 2025-06-17

Item	Qty	Tax Incl Amount
N/A	1	[redacted]

Total Tax (N/A%): [redacted]
Total: [redacted]

Figure 47: 5. The wallet offers a new credential – purchase receipt.



9:41

Additional Details

Delivery Actual Delivery Time

Delivery Actual Delivery Date

Item Property Item Property Name

Item Property Value

Party Identification Id

Party Name Name

Monetary Total Line Extension Amount

Monetary Total Payable Amount

Monetary Total Tax Inclusive Amount

Purchase Receipt Tax Included Indicator

Purchase Receipt Issue Date

Purchase Receipt Legal Monetary Total

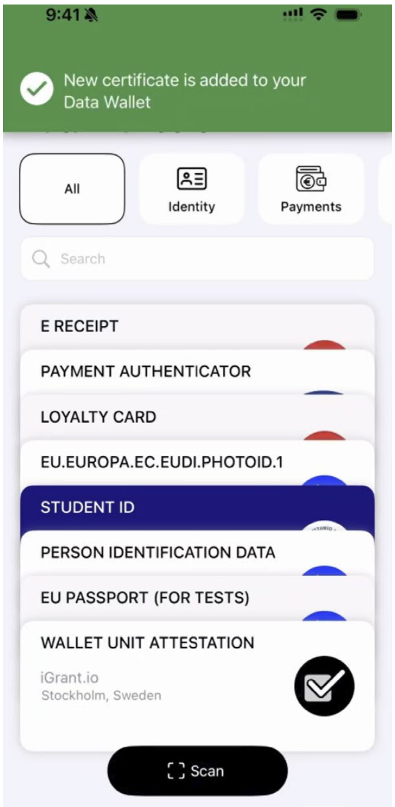
Purchase Receipt Payment Authorization Id

Purchase Receipt Payment Transaction Id

Purchase Receipt Payment Paid Amount

Purchase Receipt Id

Figure 48: 6. User can view the receipt contents.



9:41

New certificate is added to your Data Wallet

E RECEIPT

PAYMENT AUTHENTICATOR

LOYALTY CARD

EU.EUROPA.EC.EUDI.PHOTOID.1

STUDENT ID

PERSON IDENTIFICATION DATA

EU PASSPORT (FOR TESTS)

WALLET UNIT ATTESTATION

iGrant.io
Stockholm, Sweden

Figure 49: 7. The receipt has been received in the wallet.

Annex B: User Testing Feedback

Open a bank account – Digital Wallet Trial User Feedback form

Thank you for participating in the user testing and helping to develop a new type of digital EU identity wallet for business. With this survey, we want to collect your experiences and views on the different stages of testing. Your feedback is invaluable in order for us to improve the service and ensure its ease of use and functionality.

Answering the survey will take approximately 10-15 minutes, and all responses will be treated confidentially. The survey asks about your experiences using the application, the smoothness of the testing process, and your possible development suggestions

1. How easy was it to install the mobile application?	
Very difficult	**Very easy**
2. How easy was it to load the user profile into the mobile application?	
Very difficult	**Very easy**
3. How clear were the instructions provided for the demo?	
Very unclear	**Very clear**
4. How satisfied were you with the test bank's user interface design?	
Very dissatisfied	**Very satisfied**
5. How easy was the authentication process in the test bank using the mobile application?	
Very difficult	**Very easy**
6. How easy was opening an account overall?	
Very difficult	**Very easy**
7. How easy was it to transfer your company's certificates to the bank?	
Very difficult	**Very easy**
8. How would you rate the speed of the whole process?	
Very slow	**Very fast**
9. How secure did using the test bank feel?	
Very insecure	**Very secure**
10. How confident did you feel when using the application for cross-border banking?	
Not confident at all	**Very confident**
11. When using the test bank, did you understand the purpose of the different intermediate stages?	
I didn't understand them very well	**I understood them well**
12. How would you rate filling in the business wallet address in the test bank?	
Difficult	**Easy**
13. How satisfied are you with the test bank in general?	
Not satisfied at all	**Very satisfied**
14. How likely would use similar wallets for cross-border banking?	
Very unlikely	**Very likely**
15. How likely would you recommend the tested model for opening an account to others?	
Very unlikely	**Very likely**
16. What additional features would you like the application or the test bank to have?	
17. What additional instructions or support would you have needed during the testing?	

18. What other observations did the use of the application and test bank raise in you?	
Think about a time when you have, outside of this trial, tried to open or opened a bank account for a business, and answer the following questions. Answer based on your actual experience.	
19. I have previously opened, or tried to open, a bank account for a business:	
in my home country (please specify which country):	
abroad (please write which country):	
I haven't tried or opened a bank account for a business:	
20. What would have been your opinion at the time you tried, or opened, a bank account in a different country on the statement "opening a bank account for a business is easy"?	
Completely disagree	**Completely agree**
21. In what role did you act in the company at that time?	
owner	
CEO	
financial manager	
accountant	
accounting firm representative	
authorized signatory	
other, what?	
22. What was the form of operation of the organization in question?	
sole proprietorship **general partnership**	
limited partnership	
limited company, corporation, LLC etc.	
cooperative	
tax consortium	
association or foundation engaged in business	
other, what?	
23. How many employees did the organization employ?	
0-9 employees	
10-49 employees	
50-249 employees	
over 250 employees	

Create a company branch – Testing

All service or product development, be it physical or digital, should always include at least some collaboration or discussion with the different user groups intended to use the product or service. Creating completely new concepts using completely new technologies, makes the testing more delicate and difficult, yet even more important. Experience gives us that what you, as a developer or a representative of the organisation developing the service, think are the most important things to solve, do not necessarily correlate with the user experience.

Background

The registration of a Norwegian-registered Foreign Company (NUF) is one of the most important processes for foreign businesses wishing to operate in Norway. This provides them with an organisation number, which is the foundation for all other actions they need to take in Norway – invoicing, registering employees at a workplace (HMS card), and submitting VAT and taxes. However, the process is often perceived as time-consuming, complex, and characterised by manual steps. This creates frustration among users and can lead to delays and unnecessary costs. Errors in documentation and a lack of understanding of the requirements are amongst the most common challenges, resulting in many applications being returned for correction.

With increasing demands for digitalisation and user-friendliness, there is significant potential for improvement. Users are requesting solutions that can make the process simpler and more efficient, with a particular focus on better guidance and increased use of digital tools. Their wishes include automated validation, digital signatures using BankID, and a clearer and more logical layout of forms.

Questions asked to users

In the case of using digital identity wallets to identify you as a person or a company, and to share information in a secure and trustworthy way, we wanted to understand the users' perception of the create a company branch flow focusing on a number of areas and questions:

- Does the user understand the task and how to carry through with it (going through a number of steps to apply for, claim and share digital attestations, and to register a company branch)?
- Is there enough information about the concept of digital identity wallets, attributes, security, trust and the flow between different countries and devices for the user to understand it?
- The issue of trust – does it feel secure and safe?
- Is this way of creating a company branch easier than the current one?
- What is the experience switching between the different parts of the flow (starting by finding how to create a company branch in Norway, applying for an NPID, issuing an EUCC in Sweden and finalise the application, using the digital identity wallet sharing credentials, in Norway)?
- What is the experience switching between different devices?
- What would make the experience smoother?
- What should be changed?

It is equally important to understand the pains and needs of the users intended to use the service before starting designing and developing, as it is testing the designs and developed services. The user groups consist of both external and internal users of the system, and by mapping the different groups gaps and uncertainties in the current process can be taken into account for future development. Initial in-depth interviews gave that understanding for designing the create company branch process.

Target group and implementation of tests

The majority of company branches in Norway with a registered Swedish mother company, is in the SME sector. The create company branch pilot is partly built to serve these companies, but as larger companies applying for branches use external professional representatives of the mother company, these were included in the tests as well. Figure 50 and Figure 51 show the country of origin of mother company for branches in Norway and Sweden.

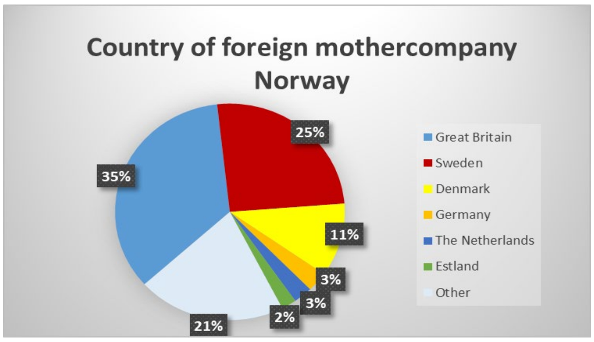


Figure 50 Country of foreign mother company Norway

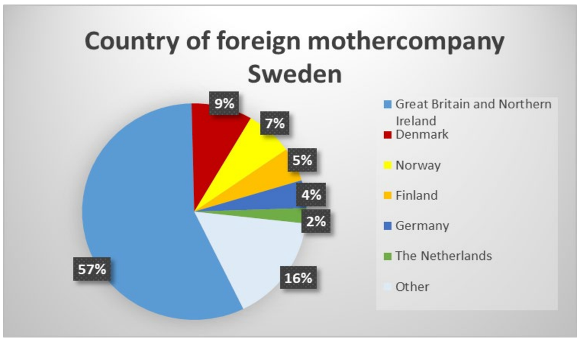


Figure 51 Country of foreign mother company Sweden

The create company branch pilot is yet in an experimental phase of using digital identity wallets (especially for organisations), however it is important to find out both how the concept of using digital wallets for information sharing cross-border, and how new forms and ways of applying for a company branch works for the user. Whereas the concept is new, it could be tested on almost any private person, despite not representing a company. In that case, the emphasis is not in understanding how to fill out an application form, but to understand the concept of digital identity wallets and attestations. The experimental stage of the development of a service also implies for quick answers and adjustments, which is why the number of user test could be limited to a few. Experience also tells us that the most important feedback of a concept or a service will be detected even with a small number of user tests.

As the pilot is developed in a controlled test environment, tests on the actual technical solutions could only be carried out in physical tests on a trusted network. Tests with “real” users had to be performed using Figma prototypes (clickable images of the flow), hence limiting the real experience of shifting devices.

The tests ran at three different occasions, where the first part was to uncover needs in today’s service for registering a company branch and to get inspiration as to how the future service should look like. The second part, testing the designed and developed pilot, was carried out at two different occasions, giving the opportunity to adjust the design to some of the feedback between the first and the second test opportunity.

In-depth interviews November 2024

- 5 interviews with consultants (video meeting)
- 1 interview with case officer employed by Brønnøysundregistrene (video meeting)

User test occasion 1 – 12 March 2025

- 3 physical tests with employees from Brønnøysundsregistrene.

  - 2 test persons with no experience from digital identity wallets
  - 1 test person with knowledge of the semantics used in attestations
- 3 digital, remote, tests (with Figma prototypes) with external users that work with creating company branches in their profession

User test occasion 2 – 31 March and 4 April 2025

- 5 digital, remote, tests (with Figma prototypes) with employees from Bolagsverket, Brønnøysyndsregistrene and one external user
  - 2 test persons from Bolagsverket with no experience from digital wallets
  - 1 test person from Bolagsverket with experience from previous work on digital wallets, but not working with EWC
  - 1 test person from Brønnøysundsregistrene that also participated in user test occasion 1
  - 1 test with external user that work with creating company branches in their profession, that also participated in user test occasion 1

Applying for a company branch in a foreign country – testing the different steps of the process

Several parties are involved in the process of registering Norwegian-Registered Foreign Enterprises (NUF), including accountants, lawyers, advisors, and company representatives. NUFs are often established for short-term projects in Norway, particularly in the construction and civil engineering sectors, but also for specific purposes such as insurance or other business activities.

The registration process involves submitting documents to the Brønnøysundsregistrene, which requires a significant amount of manual work. Generally, two-thirds of the application pertains to registration in the Central Coordinating Register for Legal Entities, while approximately one-third involves registration in the Register of Business Enterprises.

The designed and developed prototype is limited in its scope and based on a so called happy case, where everything run smoothly and no errors occur. In this case, there are some preconditions for the service to work, not necessarily coherent with how it would work in reality. For example, to consideration is taken to the different registers.

Preconditions for the test

The users testing the service were given information on what role to play in the test, and the preconditions for the company they represented:

- A Swedish company wants to start a branch in Norway.
- The Swedish company has an EUID, equivalent to a Norwegian limited liability company such as AS, ASA, or SE.
- The Swedish company has no address in Norway.
- The company registers for the first time in the Register of Business Enterprises.
- The Swedish company has a general manager which is also the applicant. The applicant has a Norwegian national identification number, is liable for an NPID and has a digital wallet.
- The applicant is the general manager/submitter/fee payer and contact person, as well as the sole board member/chairperson of the company. Therefore, he or she has the signatory rights for the company.

The different steps in the create company branch flow tested by users is shown in Figure 52.

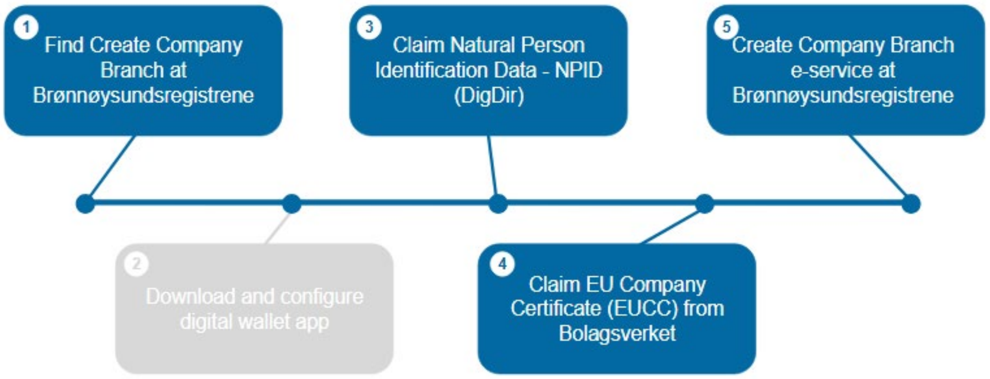

1 Find Create Company Branch at Brønnøysundsregistrene
2 Download and configure digital wallet app
3 Claim Natural Person Identification Data - NPID (DigDir)
4 Claim EU Company Certificate (EUCC) from Bolagsverket
5 Create Company Branch e-service at Brønnøysundsregistrene

Figure 52 Steps in create company branch flow

Step 1: Find Create Company Branch at Brønnøysundsregistrene

The user's main goal in this step was to find the correct website to begin the create company branch application process. Currently, users will find an information page on the Norwegian government site Altinn.no when searching for "create branch" in Norway. We used this as the main page and edited the text, as well as created an additional "homepage" for the service. This homepage is intended to give users an overview of what is required to complete the create branch application, including links to the different websites needed to collect attestations and download the wallet app. For the last test we deleted the Altinn page, as this created more confusion than it helped, and added a page between the start of issuance process to help the user navigate to the right country/organisation that will issue the right attestation.

Recommendations for future development

- Users want simpler and clearer descriptions. For example, spelling out "EUCC" as "EU Company Certificate," makes it easier to understand.
- Most users did not read much and clicked through the pages quickly. A lot of information was missed. Users assumed they did not need to read because:
  - They had done similar tasks before and believed they already knew what to do.
  - They expected the system to stop them if something went wrong.
- In the fully developed service, there will be need for letting the user find its country and the organisation(s) that have the issuance process for several different attestations. The coordination of this page should not be national but ideally run by the EU.
- How detailed and country-specific should the process be? The difference in how to get an attestation between the different organisations is confusing to people, as they need to learn how to navigate several sites. The look and feel, and the process itself should be more standardised.
- How can we ensure applicants understand what preparations are needed before they fill out an application form? One way is to create a test for your wallet to see which attestations you are missing (this is already an available feature in iGrant's solution)
- What differences are there between consultants and company owners applying? Today, many applications are submitted by consultants handling financial services in Norway. Our current flow is designed for the less common case, where the owner completes the application.

Step 2: Download and configure digital wallet app

Applicants were sent to App Store/Google Play to download a wallet application. This step is out of our control, and there may be multiple wallet apps available in the future. We did not go

Co-funded by the European Union

through this step in the user test but assumed the wallet app was already installed and configured. However, there are some general feedback on the wallet app.

Recommendations

- Uncertainty remains about where to lead users in app stores if we cannot direct them to a specific app.
- Leave technical language out of the user experience. None of the users understand what "Wallet Unit Attestation" means.
- The user experience in the wallet app is key for understanding how and why and where to use attestations. Confusing experience with the wallet app language and interface will lead to low adoption. Authorities need to have some control as how the attestations are presented. The wallet app we used for the create company branch pilot use the default layout and setting, and does not present a very well thought through user-experience.
- To activate the app, users need an NPID or LPID. This is currently handled in a later step (Step 3), but ideally, it should be integrated into the same flow of downloading wallet-app.

Example of user problems

- Users did not understand what the attestations were, i.e. the difference between the NPID and EUCC. Everything was presented in the same way. Even though NPID felt more like private data than EUCC.
- Data fields were greyed out and hidden. Which was confusing for users as they believed they were supposed to fill out the blurred fields. Users did not understand that information was hidden behind the “eye” icon. Users were reluctant to accept something they could not see.
- Newly claimed attestations appear at the back of the stack, making it hard for users to notice the most recently updated attestation.

Step 3: Issue Natural Person Identification Data - NPID (DigDir)

To validate the wallet, the user needs to download the NPID attestation. This attestation also includes data required for the create company branch application.

In this pilot, the attestation was issued by Brønnøysundsregistrene, because the NPID attestation from DigDir is not compatible with the iGrant wallet. Normally, Norwegian applicants would receive the NPID from DigDir or Skatteetaten. If the applicant is from another country, they must obtain the attestation from their national authority issuing NPID’s in that country.

Recommendations

- It will be challenging to direct applicants to the correct issuer, especially since Brønnøysundsregistrene does not know the applicant's country of origin.
- None of the users understood what an NPID is. It must be understandable for the user what each attestation contains, who is responsible for issuing it, and what organisations it can be used for.
- Use consistent terminology across platforms and services, the language from issue NPID was different than the language for issue EUCC and this is confusing. There should be standard descriptions used across the EU.

Step 4: Get EUCC from Bolagsverket

Users were asked to log in to Bolagsverket using a foreign ID via the EIDAS-node (managed by DigDir) and to select the EUCC attestation, which they then downloaded to the wallet app.

Recommendations

- Test the user experience using low-fidelity sketches before technical implementation.
- Avoid creating steps that do not match user expectations.
- Language needs to be consistent across borders and platforms.
- Bolagsverket's solution requires that the user logs in to access information on the company and to claim different attestations. The user then anticipate a more personalised presentation of information.

Step 5: Create Company Branch e-service at Brønnøysundsregistrene

In this step, users shared attestations with Brønnøysundsregistrene. These attestations are used to prefill parts of the application form. Users filled out the remaining fields, signed the application using the wallet app, and could download a receipt to the wallet app after the application was done. We changed texts in the forms between occasion 1 and 2, based on the feedback we received. At the second occasion, the language was easier to understand and more aligned with user needs/expectations than it was during the first user test.

Recommendations

- Written content needs to be precise and aligned with the process. If users think they need to fill out a field, they will not be interested in reading about the process.
- Users should be nudged to identify where information is missing.
- Clarify where prefilled data comes from.
- Make it clearer that information in the form cannot be changed—users must return to the attestation issuer (the origin source of the information).
- Users appreciated that the form had limited choices and follows legal requirements.
- The most common scenario is for an external representative to submit the application. Today, a copy of the CEO's (or similar) passport is needed. This has to be handled in a future solution.
- Users assumed that submitting attestations meant they were logged in. As this is not the case, scanning the wallet app to sign and download a receipt felt unnecessary.

Results of the user tests

Even though users struggled a bit in understanding the concept of digital identity wallets and the toggling between different sites, countries and devices, there were a lot of positive reactions to this new process:

- *"The registration doesn't need to be more difficult than this!"*
- *"Good that it is so easy. Case handling only takes time and stops companies from doing business in Norway as they don't get a Norwegian company number."*
- *"This is 10 times better and more efficient than today."*
- *"Even a person that have never created a branch could do it here, but you need to know what credentials should be shared." (Today's process is described as only for experts)*
- *"100 percent the right way to go! Get rid of all the paperwork!"*
- *"Would have been good if creating a branch was this quick."*
- *"This flow makes it more secure than today, as everyone needs to identify themselves."*

Key findings and considerations

- **To visualise expectations and help the user understand what to do and where they are in the process is key for success.**
    - Users felt uncertain about where they were in the process, what each step contained and what type of action was expected of them. They were asking for

Co-funded by
the European Union

    - visual information that could confirm that they had done the right thing. For example, the possibility to test if you have all the needed attestation before you start the process was highly welcomed by the user.
    - The homepage was seen as helpful, but it was unclear for the user as to how to return to it as they navigate between a lot of different pages to fulfil all the criteria for the process.
    - It is also important to consider making a common page that collects all necessary web addresses for the different issuing processes for each use-case/attestation. This should preferably be centralised and handled by the EU and not each country. The need for a centralised issuance guide will be reduced if the user does not need to collect the attestations single-wise, but instead there is a solution for “batch-issuance” of all the attestations available when you create a company wallet.
- **The “create company branch registration” process is better with using digital attestations than paper-attestions and registration form on paper, and will lead to better data quality in registers.**
    - By transferring the manual process of today to a complete digital process and reduce the case handling time to possible minutes or seconds made users enthusiastic.
    - The simplicity of the process makes it possible for more people could handle it without extensive training or experience compared with today. Even the consultants helping clients today could envision a service where the client did this process themselves.
    - Users saw that this process is more secure than today and that the data shared would be of higher quality in the future with a system like this.
    - This way of designing registration-services will lead to better data quality in registers as we force users to correct wrong information in the attestations.
- **There is a strong need for plain language.** Users struggled to understand the terms, their meanings, and what data was being shared with whom. Language and abbreviations are seen as cryptical for people with no experience from the terminology.
- **The overall concept of digital wallets, proofs, and trust infrastructure is difficult to grasp.**
    - Some of the user reacted negatively having the role as middle-men in a process they think authorities should handle and that there should be a common European registry that contains all relevant data from every national registering authority.
    - Others perceived the attestations (in this case the EUCC and the NPID) as just a pdf, and was happy that the tested service moved away from paper. They did not understand the trust infrastructure behind the attestations. This emphasise the importance of adoption and envisioning the value behind the e-ID/wallet technology in a clear and precise way. Who will be in charge of getting adoption in a country? However, users believe their understanding of the value of wallets and how to use them will change as they get more used to using them. It is hard to understand what attestations to use for what and why. Today the attestations are collected from a variety of organisations that each has its own flow and this makes in hard and confusing for the user to understand their function.

Citations from the tests:

- *“This is a practical flow, but feels like an advanced form of copy-paste.”*

- *"It's just a digital PDF."*
- **Too many QR scans and transitions between devices and "places" makes navigation harder and raises security concerns.** Staying on one device improved usability compared to going back and forth between a website and an app. The switch between surfaces using QR codes feels unnecessary, and some users are uncomfortable using them. As so called quishing (using false QR codes for criminal use) increase in public places, people are told to be careful scanning them as the security around QR codes is debated.
- **Trust and security are closely tied to the role of the organisation that ask for the attestations.** Despite the confusion around wallets and how they work, the services were generally perceived as secure and trustworthy. The reason is because they are tied to public authorities. In the case of the user tests, the cultural context most probably plays a role, as the Nordic countries considers public authorities inherently trustworthy. This affects the adoption of the concept, but the question is how this trustworthiness can be transferred to private organisations and countries with another cultural setup?
- *"If it weren't public, I wouldn't trust it."*
- **There is a need to find solutions for representations and signatory rights.** Cultural and organisational hierarchies will influence speed of adoption and how the service is used.
  - Where the administration of representations and signatory right in a business will be handled is key for making successful digital wallets services. Questions on what data will be stored, when (using the wallet or in another way) and where need to be addressed.
  - Users raise concerns that it might be hard to make less digitally mature countries to become completely digital in this process, as they trust a paper-based process. We were told executives will never sign digitally themselves, but get others in the organisations to do it for them (this is how it often works in today's analogue process).

General recommendations for future testing and development

The EWC work has mostly focused on technical frameworks and solutions, and legislative issues, given little room for or interest in the actual intended user of the services, his or her experience and the problems the user encounters. Whereas legislation, standardisation and technological solutions is the foundation for actually getting cross-border interoperability and secure services to work, the understanding of the user's gains, pains, driving forces and preferences should be the common focal point in what problem solving to aim for. This helps us work with a common goal and avoiding diverging solutions depending on the individual interpretation of the task.

Focus should be on adoption

The goal should be for the pilot to be understandable and easy to use for the target group, letting technology be developed not only to support legal and interoperable issues, but also driving the change from today's to tomorrow's solutions. Development framed around adoption includes things as:

1. **User-centred design**: Development should focus on understanding user needs, pain points, and behaviours to create solutions that are intuitive and valuable.
2. **Onboarding and training**: A well-designed onboarding process helps users quickly understand and start using the service, increasing the likelihood of adoption.

3. **Measuring adoption**: Tracking key metrics such as time-to-value, usage frequency, and user feedback is crucial for evaluating the success of adoption.
4. **Continuous improvement**: Adoption requires an iterative process where the service is adapted based on user feedback and data analysis to optimise the experience.

In the development of a pilot, all steps might not be carried out in full but should still be tested and included on a smaller scale.

Suggested way of working for future projects

Using service design as a starting point to discuss and align the understanding of a task, including the scope and the receiver of the result, is a well-known, research-based and commonly used method for developing digital services, but could (and should) also be used in the creation of POCs and pilots. This also includes the focus on the adoption of the service.

According to the ARF-design principles: ARF 1.8, chapters 4.2 Design principles and 4.2.1 User-centricity, the EUDI Wallet should be built on four key design principles — user-centricity, interoperability, privacy by design, and security by design — that guide its development to ensure compliance, usability, and trust. These principles should emphasise intuitive interfaces, seamless cross-border functionality, robust data protection, and transparency in data sharing. By prioritising user needs and embedding privacy and security into its architecture, the wallet would foster trust, encourage adoption, and align with the goals of the European Digital Identity Regulation to create a secure and inclusive digital identity ecosystem.

Much of the work carried out in the EWC has focused on interoperability, privacy, security and technical framework and solutions, but lack the usability and user-centricity. In future projects, all parts needs to be equally addressed in order to secure a successful adoption of new ways of handling identities and different attestations.

For the pilot to serve as a successful and useful base for future development of fully implemented services, different disciplines need to cooperate and collaborate throughout the project. The emphasis on the different areas (user experience, legislation, technology etc.) will vary over time, but all aspects need to be a part of the overall design at all times.

There is a sweet spot for successful innovation illustrated in the Venn diagram show in Figure 53. By letting technology, user experience and legal aspect have impact on the decisions in the development process at all times, we can overcome cultural differences between different professions (and cross boarders) and have a clear focus on the goal and end result. With a truly user-centered way of work, we are curious on other professional areas, treat all areas as equally important for the whole. And we also let all disciplines comment on each other’s work.

"If you only focus on the engineering side, the project ends in a rabbit hole"- Tech provider

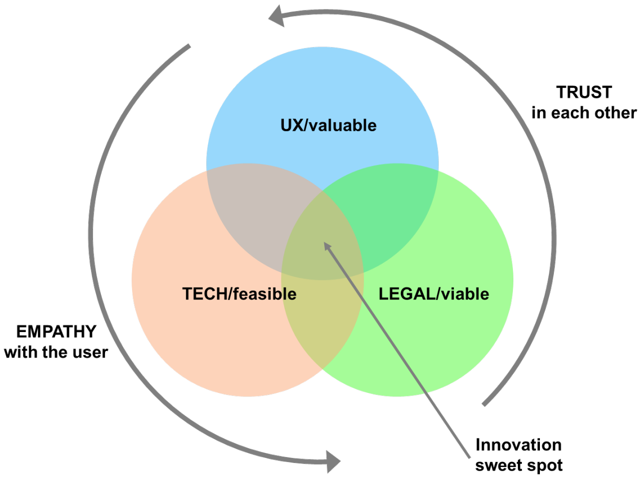


Figure 53 How to collaborate between different disciplines and areas to reach the sweet spot of innovation

Brønnøysundsregisterne and Bolagsverket have worked with slightly different approaches on including design thinking and user feedback in the concept and technology development. Whereas Bolagsverket focus has been on the technical framework, taxonomies and to build back-end solutions that strive for interoperability between systems, Brønnøysundsregisterne have had more emphasis on using user-centred design as the main starting point in the EWC Create Company Branch business scenario. As Brønnøysundsregisterne started the work on the create company branch service, focusing on the registration forms, user testing, learning from the feedback, and changing user interfaces and flows accordingly, were carried out late in the project. Nevertheless, the user experience increased with the implemented changes jointly carried out by Bolagverket and Brønnøysundsregisterne in mid-March and early April, and there are learnings to bring into future work.

In order to use the insights gained now, both from the actual user tests and from the non-optimal way of working throughout the project, the following is suggested as an easy-to-use guide for a way of work for the coming consortiums:

The way to start a project

1. Start out by sketching your dream scenario.
   If everything ran smoothly, what would you like a user to achieve after going through the end-to-end flow? Who is the user? What role does he or she have when using the services: is it a private person, an entrepreneur or a professional? Or all of them?
   Include specialists from different parts of your organisation(s) is this process.
2. Create the business case with components and insights from step 1.
3. Start user testing the concept early. Already when it is no more than a vague idea. And continue testing, on small groups, throughout the development process.
4. Think about what information, training, campaigns etc. are necessary to carry out to make the new concept and service understandable. Is it intuitive enough to stand alone (like the interface of the first Apple iPhone), or do we need to create the understanding in another way?

Co-funded by
the European Union