Dissemination level: Public

EWC D1.5

FINAL REPORT

WP 1

Author: Swedish Companies Registration Office/Bolagsverket (SCRO)

Contributors: Intesi Group, VM, GenDigital, SICPA, UPRC, Signicat & Annet Steenbergen

Day of submission: 31/07/2025

Contents

Co-funded by
the European Union

Revisions

Version	Date	Author	Changes
v1.0	31/07/2025	SCRO	Final version reviewed and agreed by contributors. Under review of Project Coordinators.

Co-funded by the European Union

1. List of abbreviations

Acronym	Explanation
(Q)EAA	(Qualified) Electronic Attestation of Attribute
EAA	Non-Qualified Electronic Attestation of Attribute
Pub-EAA	Public Body Electronic Attestation of Attribute
ACM	Access Control Mechanism
ARF	Architecture and Reference Framework
CBOR	Concise Binary Object Representation
CIR	Commission Implementing Regulation
COSE	CBOR Object Signing and Encryption
DTC	Digital Travel Credential
EDIR	European Digital Identity Regulation
eID	electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
ETIAS	European Travel Information and Authorisation System
EUDI	European Digital Identity
F2F	Face-to-Face
FAQ	Frequently Asked Questions
FAR	False Acceptance Rate
FRR	False Rejection Rate
IBAN	International Bank Account Number
ICAO	International Civil Aviation Organization
ISO	International Organization for Standardization
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
MRTD	Machine Readable Travel Documents
NFC	Near Field Communication
PAD	Presentation Attack Detection
PAN	Primary Account Number
PID	Person Identification Data

Co-funded by
the European Union

Acronym	Explanation
QC	Qualified Certificate
QES	Qualified Electronic Signatures
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
SD-JWT	Selective Disclosure for JWTs (JSON Web Tokens)
SOG-IS	Senior Officials Group - Information Systems Security
T&Cs	Terms and Conditions
TSP	Trust Service Provider

Co-funded by
the European Union

2. Introduction

Over the past two years, the EWC project has brought together public and private sector institutions in a collaborative effort to shape a practical and sustainable EUDI wallet ecosystem. Focusing on travel, payment, and business use cases, the project has consistently prioritised **real-world applicability** and **stakeholder engagement**.

The project consortium embraced a **pragmatic and solution-oriented philosophy** that ensured external dependencies, such as delays with the ARF delivery, did not hinder progress. By emphasising strong **public-private collaboration**, we created space for viable **business models** that are essential for long-term ecosystem sustainability.

Our approach targeted **high-frequency, high-volume use cases** to ensure the EUDI Wallet becomes a tool of everyday value for individuals and organisations alike. Continuous engagement with key stakeholder communities enabled the development of solutions that **align with existing systems** while delivering clear added value. A strong emphasis on **usability and user experience** guided our pilots, ensuring that the EUDI Wallet can meet or exceed the expectations set by current solutions.

Together, these guiding principles have helped lay the groundwork for a functional, inclusive, and scalable EUDI Wallet ecosystem that reflects the needs and realities of both the public and private sectors across Europe.

Co-funded by
the European Union

3. Overview per WP

This chapter presents a concise summary of the key results from EWC for each work package.

3.1. Work Package 1 – Project Management & Coordination

Work Package 1 has played a central role in ensuring the successful execution of the EWC project. Through strong coordination, structured processes, and continuous oversight, WP1 has enabled the project to stay aligned with its budget, timeline, and strategic objectives, while remaining adaptable to evolving requirements.

Key project management activities were formalised and governed through a living Project Management Handbook, which provided a clear and updated framework for day-to-day operations. Strategic oversight was ensured via regular Management Board meetings, while cross-functional coordination was facilitated through structured engagement with work package leaders as part of the regular Work Package Leader meetings.

A strong focus was placed on stakeholder alignment and transparency. The Member State Advisory Board (MSAB) served as a key forum for gathering input from national representatives, ensuring the project remained relevant and responsive to Member State priorities. Additionally, WP1 successfully organised the project's kick-off and General Assembly meetings, fostering cohesion and alignment across the consortium.

WP1 also ensured timely and accurate financial and technical reporting, including internal interim financial reviews and the successful facilitation of the project's formal interim review in autumn 2024. The work package acted as the main interface toward the European Commission, HAdEA, DG CNECT, and other relevant Directorates-General, ensuring effective communication and coordination with institutional stakeholders. WP1 also facilitated collaboration with other Digital Europe Programme-funded LSPs, contributing to a more harmonised and informed implementation landscape.

To ensure delivery quality, WP1 produced and monitored the project's Quality Assurance Plan, oversaw the preparation and timely delivery of project deliverables, and continuously assessed and updated the project's risk posture through a living Risk Catalogue aligned with the Risk Management Plan.

Legal and administrative coordination was also a key function. WP1 provided legal support to partners and prepared the project's Consortium Agreement in line with the DESCA guidelines. It also led the coordination and execution of several Grant Agreement amendment rounds, ensuring the project remained aligned with evolving needs and priorities.

In sum, Work Package 1 has provided the operational backbone of the project, enabling effective collaboration, risk management, and quality assurance across all levels of the consortium. Its work has been fundamental in ensuring the project's delivery in line with the grant agreement, while maintaining agility and alignment with the broader goals of the European Digital Identity initiative.

Co-funded by the European Union

3.2. Work Package 2 – Digital Travel Credentials and Payment Use Case Applications

Introduction

WP2 is about taking the EWC wallets (WP3) and infrastructure (WP4) and implementing those specifically for the travel and payment use cases along the travel journey.

To demonstrate how

- The EUDI wallet can automate manual processes for people, organisations and governments.
- Organisations can reduce time and effort to comply with regulations related to organisational identity.
- Payment services contribute to scaling the EUDI wallet.
- The EUDI wallet gives citizens confidence to interact online by securing the user journey and verifying that they are dealing with genuine organizations not scammers.
- The EUDI wallet makes the EU more attractive as a travel and tourist destination and enhances inter-EU commerce.

And to explore

4. Interoperability challenges across Member States and 3rd countries
5. How payment services can benefit from using the EUDI wallet in terms of user experience, innovation, security, and fraud - and explore impact on existing standards, business models, and infrastructure.

Travel and payment industry EUDI wallet related analyses

To define the travel journey and issue verifiable credentials (T2.1) and to issue payment credentials and issue payments (T2.2) the workpackage participants explored the context in which the EUDI wallet must be implemented by analysing state of the art technology, regulatory requirements and business incentives. Key results are captured in several deliverables, white papers and videos:

1. Deliverable 2.1: Digital travel Credentials (SICPA). On top of PID, the travel and payment industry requires the EUDI wallet to provide passport attributes (like passport number and picture) to fulfill regulatory and business requirements. Four options leveraging ICAO DTC and the ISO PhotoID have been explored.
2. Deliverable 2.2: Booking of Travel and Stay (Amadeus). Similar to D2.1, the initial finding of the study indicates that the primary value in utilizing wallets during booking processes arises from the ability to verify information beyond the Personal Identification Data (PID) of the wallet holder. Furthermore, the presence of a certified portrait picture, valid for identity verification, is essential wherever there is a need to confirm that the individual who previously submitted the information online is the same person requesting the service in person.

Co-funded by the European Union

3. Deliverable 2.3: Automation of passenger information (Amadeus). Highlights the importance of OCR, NFC, and digital credentials in ensuring compliance with regulatory requirements, enhancing security, and improving operational efficiency and assesses use cases including the automation of filling advance passenger information, issuing and presenting boarding passes, and guest forms. Accurate passenger information collection is crucial for a smooth check-in process and overall passenger experience. The future vision involves passengers interacting directly with government authorities to provide travel information, leveraging digital identities and decentralized systems. This approach aims to enhance data accuracy, security, and compliance while reducing the burden on airlines.

4. Deliverable 2.4: Passenger flow facilitation (Amadeus). Present a status and future trends for passenger flow facilitation, particularly in the context of travel and border control. The report highlights the integration of biometric technology within the passenger flow facilitation and the importance of Privacy and Inclusivity, Digital Identity and Traveler-centric Solutions.

5. Deliverable 2.5: Payment enablers (Visa). Continued industry cooperation, technical refinement, and regulatory alignment are essential in the next LSPs to achieve commercial-scale deployment and realizing the vision of a pan-European digital payments authentication and initiation solution.

6. Whitepaper: What does it take to use the EUDI wallet for payments? (Visa). Facilitating payments is an important use case for the EUDI wallet and is likely to drive consumer adoption. However, payment services rely on critical infrastructure and are subject to significant regulatory requirements and certifications. Failures have a major impact on the daily lives of people and businesses. Fraud is a huge challenge while consumer acceptance and adoption rely on balancing security with a seamless user experience.

7. Implementation guide: SCA for payments using EUDI wallet (Visa). This document describes the functional specifications of the EUDI Wallet for registration and implementation of SCA (Strong Customer Authentication) using the EUDI Wallet in both card and account online payment use cases.

8. Video: EUDI wallet explainer (Gen Digital). Introducing the concept of the EUDI wallet in context of travel and payments to the general public in a clear and understandable way.

Pilots and end-user research

To run the pilots and gather end user feedback (T2.3) the workpackage defined several phases for piloting, designed and developed use cases, and onboarded relying parties (T2.4).

Under the leadership of the use case owners Visa, Amadeus, UAegean, RDE and SICPA several use cases with clear business incentive and combining travel and payment credentials have been designed, developed and piloted. Namely, use your EUDI wallet to:

- Buy a ferry ticket, including identity verification and payment, and store your Boarding pass and eReceipt.
- Confirm your age when buying a museum ticket to pay the right price, store your ticket and present your ticket when entering the museum.
- Provide your passenger information when checking in for a flight and to provide consent to the airline to use your picture to improve your passenger journey.
- Fill the hotel registration form when booking or checking in to your hotel.

The citizen research and pilots were coordinated by Gen Digital and included in-depth interviews with experts, in-depth online community research (3 EU countries, 60 people), a quantitative survey (6 EU countries, 2000 people), and a video survey (18 EU countries, 9000 people) and also included three phases of piloting EUDI wallet solutions in the context of EWC use cases.

Phase	Issuers/ verifiers	Data	Credentials	Pilot setup and participation
1	UAegean CFF RDE BudaCastle Amadeus	Dummy	PID Passport	Closed pilot with 100 Friends and Family
2	UAegean CFF RDE BudaCastle SICPA Visit Benidorm Amadues	Dummy	PID Passport PhotoID StudentID Self attested	Open pilot promoted through LinkedIn with 300+ members of the general public
3A	UAegean CFF Banca Transilvania Worldline	Real	Passport PhotoID StudentID IBAN eReceipt Ticket	Closedpilot with 50+ friends and family

Co-funded by the European Union

3B	RDE BudaCastle SICPA Visit Benidorm Amadeus Lufthansa	Dummy	Passport PhotoID	Controlled pilot with hundreds of airline customer participants

The main findings and results from the citizen research and three pilot phases captured in Deliverable D2.6: Run End User pilots (Gen Digital) are:

- The EU thinks big picture - citizens think ‘what’s in it for me?’
- The most effective path to adoption is focussing on where existing solutions fall short.
- Currently only 29% of EU citizens would adopt the EDIW.
- It’s not enough for the wallet to simply meet incumbent benchmarks, it needs to redefine what a digital wallet experience is.
- Security is at the heart of the wallet’s technology, but insecurity is at the heart of citizens’ concerns.

Scepticism shadows the wallet’s promise: to set a new standard for trust in the digital world.

5.1. Work Package 3 – Wallets Application and PID/ODI

Work Package 3 objectives included:

1. Provision of piloting users in WP2 (travel and payment use cases) and WP3 (organisational use case) with **EUDI wallets for natural persons** and/or **Legal Person (organisational) wallets**.
2. Provision of piloting users with **PID**, and/or ODI (Organisational Digital Identity) which we have renamed to **Legal Person Identification Data (LPID)**, and **organisational credentials**.
3. Piloting of Legal Person Wallets, LPID and organisational credentials in different business areas (B2B or B2G) including Public procurement, Know Your Supplier, Domain holder validation, and Business documents exchange.

To achieve those objectives, WP3 “Wallets application and PID/ODI” was organized in three (3) pillars:

1. EUDI wallets for natural persons and Legal Person (organisational) wallets provision for WP2 Travel and Payment and WP3 Organisational Identity (ODI) piloting.
2. PID and/or Legal Person Identification Data (LPID) and organisational credentials issuance and verification.

Co-funded by the European Union

3. Design, implementation and execution of Business scenarios for piloting Organisational Digital Identity (ODI) – Digital Identity for Legal Persons in 4 business areas: Public Procurement, Know Your Supplier, Domain Registration and Business Document Exchange.

Note: as the terminology shifted, EWC started using the term legal person wallet and legal person identification data (LPID) instead of ODI, and now we are also using the term "business wallet".

Wallet provisioning approach

EWC decided to adopt a pragmatic and structured approach, the **Request For Comments (RFC)** process in order to address the challenges and to bridge the gap between aligning the requirements from LSP use cases, the ARF, standards, and specifications, thereby enabling an interoperable ecosystem of wallet providers, issuers and relying parties. The diagram below illustrates the EWC RFC lifecycle and its execution across the work packages (WP3, WP4, and WP2) within the EWC framework.

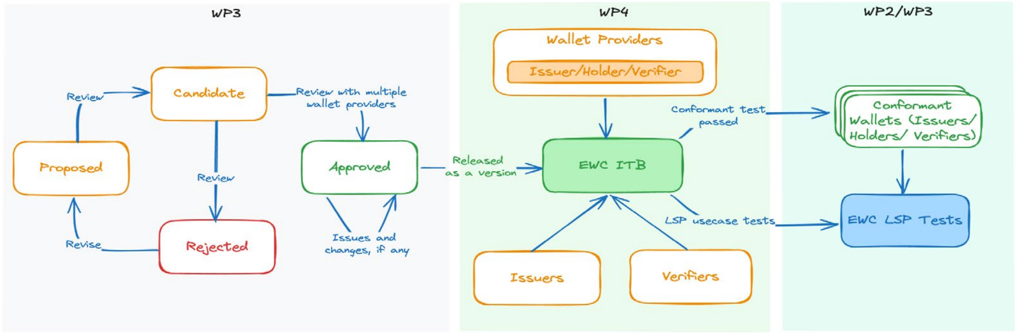

Figure 1: EWC cross-work package process

Through this structured and transparent RFC process, EWC established a clear, prescriptive stance, providing interfaces and guidelines that align with the identified requirements, including legal, architectural framework (ARF), and EWC use cases. This enabled wallet providers, both for natural and legal persons, to implement their solutions, interoperating and proving conformance through the EWC Interoperability Test Bed (ITB). RFCs are EWC community-reviewed documents which define a clear, prescriptive, and common way of implementing EUDI wallet interfaces for ecosystem participants, specifically regarding Issuer, Wallet Unit (WU), and Relying Party (RP) functionalities.

The table summarises the list of **RFCs** created during the project to build the EWC Wallet Ecosystem, which consists of Issuers, Wallet Units, and Relying Parties. These are published on the EWC RFC GitHub and depict the status as of July 2025.

Table 1*: List of EWC RFCs approved during the EWC LSP project*

RFC #	RFC Title
RFC-001	Issue Verifiable Credential - v3.0
RFC-002	The Present Verifiable Credentials Workflow - v3.0
RFC-003	Issue Person Identification Data (PID) - v2.1

Co-funded by the European Union

RFC-004	Individual Wallet Unit Attestation - v1.0
RFC-005	Issue Legal Person Identification Data (LPID) - v1.0
RFC-006	Organisational Wallet Unit Attestation - v1.0
RFC-007	Payment Wallet Attestation - v1.1
RFC-008	Payment Data Confirmation - v1.0
RFC-010	Document Signing using Long-Term Certificates - v1.1
RFC-011	Payments with Verifiable Receipts - v1.0
RFC-012	Trust Mechanism - v1.0
RFC-013	Issue PhotoID - v2.0
RFC-100	EWC Interoperability Profile Towards ITB - v2.0

The consortium went through different phases of developing and refining specifications with increasing participation over time.

Phase 01 in February 2024 delivered EWC RFC version 1.0 with five key contributors and three RFCs. Phase 02, with releases in September and December 2024 and January 2025, involved eight key contributors and produced nine RFCs. Phase 03 in May 2025 delivered version 3.0 with ten key contributors and twelve RFCs. In each phase, the ITB was available to all participants.

An **up-to-date list of RFC-compliant wallets as of EWC Phase 03**, covering:

- Natural Person Wallets;
- Legal Person Wallets (Business Wallets);
- Issuer-only and Verifier-only implementations.

is available in EWC RFC GitHub

Each solution was tested against a defined set of RFCs relevant to its role (e.g., issuance, wallet unit holder functions, and verification) and validated within the context of EWC's Large-Scale Pilot (LSP) scenarios.

The EWC approach proved to be a scalable framework that drives a multi-provider, interoperable EUDI Wallet ecosystem, rooted in transparency, collaboration, and compliance in a continuous manner. More details are included in *deliverable “D3.1 – List of available EUDI compliant wallets in EWC, and documentation”*.

Legal Person Wallet Definition and Provisioning

An important outcome of EWC was the development of the **Legal Person Wallet Definition** (part of *deliverable “D3.2 – Open-source software, hosting and documentation for the ODI wallets”*), created to fill the gap left by the absence of formal definitions in existing regulations. The EU Architecture Reference Framework (ARF) was initially developed with a natural person wallet in mind. Early in the EWC LSP, it became evident that the needs of legal entities were not adequately addressed. The concept of a *European Business Wallet*, as it was introduced in the competitiveness compass, a new roadmap to restore Europe's dynamism and boost economic growth, in January 2025 by the Commission and is now emerging, had not yet been introduced.

The definition document provides a common reference point for distinguishing legal person wallets from those intended for natural persons, as legal person wallets often require integration with internal systems and server environments, without constant end-user interaction. These differences were captured and aligned in the definition document and served as the foundation for requirements outlined below:

- **Form factor**: Legal person wallets are frequently deployed in server environments, such as on-premises or cloud-based infrastructures, often without a graphical user interface (GUI), whereas natural person wallets typically operate on mobile devices with a user-facing GUI.
- **Automation**: Legal person wallets are designed for automated operations, enabling seamless interaction without an end-user. Natural person wallets rely heavily on the end user for credential management.
- **Complexity of use cases**: Legal persons may need to integrate internal systems and processes with the wallet, such as enterprise resource planning and customer relationship management systems. Natural person wallets, by contrast, are used primarily for individual credential management.
- **Credential management and presentation**: The ability to store, manage, and selectively present credentials is a feature. Legal persons must control which credentials are shared with external parties while ensuring compliance with regulatory requirements.
- **Issuer and relying party functionality**: Each organisational wallet must support both issuer and relying party functionalities, enabling the issuance and verification of credentials.
- **Wallet Core Component (WCC)**: The wallet must support core functionalities, including communication between different wallet instances and automated exchange of credentials.
- **Cloud integration**: Legal person wallets must be deployable in flexible environments, supporting both on-premises and cloud-based installations. This is essential for organisations needing scalable, enterprise-level solutions that can integrate with existing systems and infrastructure.
- **Interoperability and standards compliance**: The wallet must comply with key standards and protocols defined in the implementing acts, ensuring seamless operation with other wallets and systems across borders.
- **Security and encryption**: Security is paramount. The wallet must implement strong encryption for both storage and communication of credentials, adhering to industry standards to protect organisational data.

Also, in close collaboration with the EWC wallet providers task and the EWC interoperability RFCs, a comprehensive set of functional requirements was identified that legal person wallets must fulfil to ensure cross-border interoperability and regulatory compliance under eIDAS 2.0.

Co-funded by the European Union

To support solution mapping and implementation readiness, a survey was conducted among wallet providers within the consortium. The responses revealed a diverse and growing set of implementations, some already aligned with the EWC definition and requirements, while others highlighted areas for further development.

These results form a basis for advancing the design, testing, and adoption of organisational wallets across EU ecosystems.

PID provisioning

The main goal that has been achieved in this task is a technical specification for PID issuance and its solution available in ITB by Member States for the EWC use cases.

The first outcome was *deliverable "D3.3 – PID country enrolment process definition"* outlining the functional aspects of the PID enrolment process, specifically focusing on natural persons. There was close cooperation between the participating Member States in order to provide the PID enrolment process descriptions of the participating countries including Finland, Greece, Sweden, Netherlands, Czech Republic and Romania.

Following the RFC process, RFC003 PID Issuance was developed describing how the PID issuance should be performed from a technical perspective accompanied with PID data schema developed using SD-JWT and OIDC4VI and aligned with the attributes specified in the PID Rulebook. Taking into account the upcoming versions of ARF and OID4VCI standard, the RFC003 was kept updated. Each version of the ARF and the first publication of the implementing act were analysed in order to provide feedback to EU commission and to OpenID foundation in order to manage technical discrepancies among ARF and tech standards.

DIGG (Sweden), GRNET (Greece), NIC.cz (Czech republic) and DIGIDENTITY (Netherlands) made available PID solution for use cases in test environment for the final testing phase of the project.

Legal Person Identification Data (LPID) and Organisational Credentials

The participation of **seven Business Registries**: Infogreffe from France, Infocamere from Italy, Kamer van Koophandel (KvK) from Netherlands, Bundesanzeiger from Germany, Bolagsverket from Sweden, Brønnøysundsregistrene (BRC) from Norway, and Finnish Patent and Registration Office (PRH) from Finland has been an excellent asset in EWC and they led the work done on **Organisational Digital Identity (ODI),** which was later changed to **LPID (Legal Person Identification Data)** and on **organisational credentials** – which are credentials concerning organisations issued by authentic sources.

The LPID attributes and generic LPID issuance process have been agreed upon by all EWC business registries and are the basis for a common LPID schema.

The table below presents the mandatory LPID attributes.

Table 2: Mandatory LPID attributes

Co-funded by the European Union

Attribute	Data element identifier	Definition	Presence (Mandatory)	Proposition and comments
LegalPersonIdentifier	legal_person_identifier	Unique id for legal persons	M	EUID (see below)
LegalName	legal_person_name	Legal person name	M	One statutory name

The EUID technical structure follows:

<country code><business register code>.<domestic registration number>_<optional validation character>

LPID definition and data schema is following DG JUST and EWC considers that **EUID is the best common identifier for legal entities** as it is an existing persistent unique identifier used in European business registers and communicated through e-justice portal, it is free of charge, the technical structure can be applied to all registered organisations within a business register (or other) and according to the Company Law Directive, business registries in Europe are already obliged to provide the EUID for certain legal forms.

Additional legal person attributes can be used as optional (e.g., LEI, EORI).

Taking into account the requirements of the business scenario pilots, the business registries worked on the following organisational credentials: **EU Company Certificate (EUCC)**, **Signatory Rights** attestation, **Ultimate Beneficial Owner (UBO)** attestation, and **Power of Attorney (PoA)** attestation.

Each registry initially mapped a proposed list of attributes to the corresponding attribute names used in their national registers, providing a basis for comparison and alignment. Following a two-days workshop, each participating country developed and refined data schemas for the agreed attestations, based on the joint work carried out during the session. These schemas served as common reference examples for use in the pilot implementation.

For the IBAN attestation, which is the only organisational credential issued by banks or open banking aggregators, a first online discussion was held by Archipels with Tink to define the scope, the rules and main attributes of the schema. After documentation work about the PSD2 and ISO standards, a data schema and a rulebook were proposed. Then a validation meeting was held with the experts of the payment use case (Tink, Visa, Wordline), and the material was slightly updated after that meeting.

The group followed the EUCC as defined in the updated Company Law Directive, and also aligned its work with the ongoing standardisation discussions within EBRA (European Business Registry Association). While the EUCC was already well-defined by early 2024, work on the EU PoA took more time and it is still work to be continued in the WE BUILD Large Scale Pilot project which kicks-off in September.

A list of the approved rulebooks and data schemas for LPIS and organisational credentials is available in EWC EUDI Wallet Rulebooks and Data Schemas Electronic Attribute Attestations GitHub

Business Registries worked also on the definition of the LPID issuance process from Business Registers to Legal Person wallet resulting to RFC005 for issuing LPID and to some piloting on LPID issuance.

Deliverable "D3.4 – ODI country schemes' definition, and organizational credentials definition, specification, and registration on infrastructure" provides a comprehensive

Co-funded by the European Union

overview of the methodology, challenges, and lessons learned in establishing interoperable and legally reliable digital credentials for legal entities across EU Member States within the framework of eIDAS 2.0 and the European Digital Identity (EUDI) Wallet.

Business scenario pilots

Starting from the 4 ODI Business Areas defined during the proposal phase and included in the Grant Agreement, different ODI Business Scenarios were submitted covering the potential digital life cycle of a business in Europe with its legal person wallet that provided requirements to pillars 1 and 2. Consequently, different beneficiaries/associated partners defined ODI pilot plans. The pilot plans were assessed according to relevance, impact, and implementation.

The ODI business scenarios, the ODI pilot plans, and the assessment of the ODI pilot plans have been included in *deliverable “D3.5 – Business scenarios pilot plans”*.

The table below presents the final state of business scenario pilot implementations.

Table 3 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

Finally, **eight** business scenario pilots (**seven** defined in deliverable D3.5 and a **new one** called “Company Authorized Business Travel and eInvoicing” added in *deliverable “D3.6 – Business scenarios pilot results and evaluation”*) were 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.

Table 4 Summary of attestations and wallets usedthe table below presents a summary of EUDI wallets and attestations used in each pilot.

Table 4 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

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**.

The findings from the pilots 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.

5.2. Work Package 4 – Interoperability and Infrastructure

Work Package 4 is the backbone of the consortium, supporting and guiding the technical implementations and providing the general infrastructure and testing for the work packages

Co-funded by the European Union

implementing the use cases. This includes quite a bit of activities that run across all work packages.

There are a number of challenges to navigate in order to create the i**nteroperability specification** for the EUDI wallet ecosystem. The actors are diverse wallet providers, attestation issuers, and verifying relying parties, from both public and private sector. Not all of them will be engaging in the same use cases or be interested in the same functionalities. Standards and specifications are subject to ongoing evolution, which can result in compatibility issues and conflicts when all participants are not able to implement them at the same speed. Furthermore, released standards often leave room for interpretation, particularly in implementation details.

EWC developed an approach on defining detailed and specific **implementation profiles** for wallet interfaces through the EWC RFCs[1]. These documents provide a definition of the wallet interfaces, based on existing standards, specifications and legislation. The EWC RFCs are combined these with definitions for data schemas, rulebooks[2] and implementation guides, which are provided by the use cases, to support the functional requirements of those use cases in testing and piloting.

All of these definitions come together in the test cases embedded in the **EWC Interoperability Testbed** (ITB), where participants in any operational role (wallet provider, issuer, verifier) can test against all the other services. The ITB provides a core conformance test suite (reflected in RFC 100 – Interoperability Profile towards ITB[3]) and various test suites supporting specific use cases or phases of end user piloting that were run in EWC. This test environment was continuously available and provided backward compatibility, so there were no strict dependencies in time or scope for participants to meet the requirements as there would have been if we would work with fixed test events or hackathons.

Based on this approach we managed to create several conformance test suites that supported each of the phases of end user piloting that we ran (see Work Package 2) and full conformance testing against the every stage of the defined specifications of our project for all participants. It also allowed us to demonstrate cross-LSP interoperability with Potential during our general assembly in Stockholm in May 2025.

We also implemented a number of **trust services** in the areas of signing and issuing of attestations. Although qualified trust services were unattainable during our project (due to the absence of specifications and certifications), we aligned to the information and standards that were available. On signing we provided an overview of the methods available for signing with the EUDI Wallet[4] and implemented signing methods based on "remote QES", which were successfully tested and demonstrated by 5 QTSPs in our consortium. Around 20 participants set up services for electronic issuing of attestations to support the use cases and we defined a rulebook and data schema to support the output for identity proofing based on ETSI TS 119 461.

[1] https://github.com/EWC-consortium/eudi-wallet-rfcs

[2] https://github.com/EWC-consortium/eudi-wallet-rulebooks-and-schemas

[3] https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc100-interoperability-profile-towards-itb.md

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

Our final set of specifications (EWC RFCs, data schemas, rulebooks and implementation guides) have **proven to work in production**. We were able to run use case pilots in all domains and even managed to execute a production flow where a real ferry ticket was purchased with a real payment in an EUDI Wallet. They provide a technical solution and a solid foundation on which the future work in the next LSPs can be based.

We believe that although not all participating wallets were able to achieve full conformance at every stage, they would eventually all have managed full conformity given enough time. This means that the profiles and specifications tested in EWC can be the basis for a successful ecosystem. It is still an open question as to how well trust infrastructure would scale, as this aspect remains largely untested.

To facilitate broad architectural discussions we organised the "**Friday Sessions**": a fixed time-slot that provided a weekly "heartbeat" for anyone to discuss tech-stack readiness, technological scope discussions, trust mechanisms, implications of updated legislation and specifications and any other topic that was of relevance to the whole consortium. Most of these were informal, with any relevant outcomes or the need for decisions or approval taken into other existing Task- or WP-meetings for follow-up. We opened up these meetings to external stakeholders and interested parties from outside EWC.

One of the topics that came out of these sessions led to our work on the **trust mechanisms and trust framework**. Our use cases in travel are very specific ecosystems in and of their own. Although they are embedded in the EUDI Wallet ecosystem and adhere to eIDAS, they also have to take into account many authorities, policies and regulation (both on national and international levels) that are not part of the EUDI Wallet ecosystem. This means that they need to rely on other existing trust frameworks and combine them with their roles in the EUDI Wallet ecosystem.

We set up an EWC Trust List[5] (as a "Third Countries Trusted List", based on ETSI TS 119 475 and ETSI TS 119 612) and created EWC RFC 012[6] for participants to be able to gain experience in working with this type of trust infrastructure. We analysed the requirements from our various use cases, who all expressed concerns on working solely with the eIDAS trust mechanisms (List of Trusted Lists and Relying Party certificates): Travel and payments (work package 2) are bound to specific legislation and authorities requiring validations and verifications outside the scope of eIDAS. The organisational use cases report the same concerns, but they also work with business wallets which are likely server-based with the capabilities to issue and verify attestations. They run into all sorts of issues when forced into the trust regime of natural person wallets. To address these concerns, we will provide a white paper with an overview of our insights from this work before the end of our project.

Last but not least, we did extensive work on **analysing the EUDI Wallet ecosystem in terms of operation, governance, trust and economics**. The key question on this was: "What does it take to get the EUDI Wallet ecosystem from the level of the EWC LSPs to start operating in production?" And preferably not merely operating, but flourishing, which means there must be real business value for all actors involved.

We analysed the governance and trust of the EUDI Wallet ecosystem based on the Trust over IP (ToIP) model. This model is developed by the Trust over IP Foundation[7], an

[5] https://github.com/EWC-consortium/ewc-trust-list

[6] https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc012-trust-mechanism.md

[7] https://trustoverip.org/

independent project hosted by the Linux Foundation. The ToIP model has been developed specifically for the design of digital trust ecosystems and represents the combined thinking of leading digital trust and identity experts around the world. We mapped the EUDI Wallet ecosystem, including all related relevant policies, legislation and standardisation bodies, to the ToIP model and identified gaps. Next, we mapped specific use cases on travel and payments from EWC to the ToIP model, including all the specific policies, legislation and entities involved there, and analysed these mappings.

We also described the economic model for credential exchange within an eIDAS ecosystem, using real use cases and participants from the EWC pilot program. It focuses on use by natural person wallet holders for credential exchange with public and private sector organisations. A key recommendation from this deliverable is to split the eIDAS economic model into short-term and long-term approaches, and to ensure that the factors that trigger the switch from the former to the latter are understood and a programme is put in place to realise those factors.

Based on the EUDI Wallet ecosystem analysis and the experiences and insights gained from all our work on implementation, testing and piloting, we will provide our recommendations on future work on implementing the EUDI Wallet ecosystem to the EC.

5.3. Work Package 5 – Communication & Dissemination

An important start for this work package has been the creation and execution of an effective communication and dissemination strategy. This initiative led to comprehensive infrastructure development, with the successful planning and delivery of key deliverables. The team implemented various communication and distribution channels actively used to engage audiences and gather valuable feedback, helping to refine and enhance dissemination activities.

One of the standout achievements was the organization of a series of lunch webinars that attracted significant participation, including between 220 and 60 attendees per session. These webinars, covering various pertinent topics related to the EWC like the Bussiness Wallet, Travel Credentials and Payments, were live events and later made available on the EWC website. These recordings, eight in total, will also be available on the official EUDI Wallet websites, extending their reach..

The EWC's presence on social media, particularly LinkedIn, witnessed substantial growth, generating approximately 200,000 views of ongoing project updates, pilots, and deliverables over the project's last year. Followers grew steadily to around 4,900, marking a successful public engagement effort. Beyond social media, the consortium's website experienced increased traffic, with 110,000 views and 46,000 visitors since its launch, providing an accessible platform for consortium introductions, deliverables, white papers, and demo videos and press releases. Next to LinkedIn EWC published RFC's, deliverables and Whitepapers on their own GitHub page.

Through a bi-monthly internal newsletter, WP 5 ensured continuous updates for EWC members, bolstering internal communication. Externally, active participation in over 90 events and conferences, webinars, and podcasts emphasized the EWC's relevance in the digital identity wallet European and international landscape. From presentations at event to

Co-funded by the European Union

interviews and podcasts many members of EWC were communicating the work of the LSP and the impact the EUDI Wallet will have on many aspects of citizens' lives and businesses.

Moreover, WP 5 facilitated collaboration with other projects and EU bodies in collaboration with EWC-members, supporting strategic alignment and interoperability within the European Digital Identity ecosystem. Regular exchange protocols were kept with international standardisation bodies, open-source communities, and global digital identity networks. Furthermore, engagements with other eID Projects and EU Bodies have also supported the alignment of the project's technical, policy, and use-case developments with broader efforts in the European Digital Identity (EUDI) ecosystem.
WP 5 played an active supporting role in coordinating four General Assemblies that brought the EWC members together. Press announcements were prepared for each general assembly and this gave the Consortium substantial media coverage.

Overall, Work Package 5 successfully orchestrated a multifaceted communication strategy that expanded the EWC's visibility, fostered stakeholder engagement, and ensured the project's lasting impact in the evolving digital identity sector.

Co-funded by
the European Union