EWC DELIVERABLE 3.5

D3.5 BUSINESS SCENARIOS PILOT PLANS

UPRC, INVINET

Dissemination Level: Public

Co-funded by
the European Union

Content

Co-funded by
the European Union

List of Figures

Co-funded by
the European Union

List of Tables

Co-funded by
the European Union

Executive Summary

Deliverable D3.5 "Business Scenarios Pilot plans" presents:

- Definition of the **Business Scenarios** that include implementation of the **EWC Organisational Digital Identity (ODI) / Legal Person Wallet within WP3 piloting**. The Business Scenarios are spread across the four Business Areas (B2B and B2G) that were identified during the proposal preparation phase and are stated in the Description of Action.
- Design and timeline of ODI **pilot plans** including the assessment of the pilots and their readiness status.

Deliverable D3.5 presents the **documentation** of the result from phase 1 "Eliciting and Representing Business Requirements and Service Design" and phase 2 "Detailed Design of the Usage Scenarios to be Piloted" of the Pilot Lifecycle, which constitute the content of piloting subtask T3.3.1 Business scenario Pilot Design within the WP3 workplan under task T3.3 Business Scenarios Piloting.

Furthermore, D3.5 provides a comprehensive overview of the methodology employed to establish business scenarios and pilot plans within the EWC WP3 piloting of Organisational Digital Identity (legal person wallets).

Starting from the **four (4) Business Areas** (Public Procurement, Know Your Supplier, Domain Registration, and Business Document Exchange) that were identified during the proposal preparation phase and are stated in the Description of Action, and utilizing an iterative approach and collaborating closely with domain expert participants and stakeholders, **eight (8) Business Scenarios** have been defined aligned with the objectives of EWC and described in detail.

Following the definition of business scenarios, participants undertook the task of formulating pilot plans, leveraging a structured presentation template. **Nine (9) pilot plans** have been provided by different EWC beneficiaries that are going to pilot Organisational Digital Identity (legal person wallets).

The pilot plans were qualified by assessing their alignment with EU and national initiatives and policies, their potential impact, and their feasibility of implementation. The pilots identified are assessed as being of good value, with good relevance to business needs and market potential.

Deliverable D3.5 is a living document that is going to be internally updated during the project duration as long as the pilot plans are evolving. The **updates** will be issued **every quarter** (September 2024, December 2024) and the last update will culminate to deliverable D3.6 including the final pilot results. As the pilot plans evolve, the next versions will track their execution until the end of the project.

Co-funded by
the European Union

List of Abbreviations

Acronym	Explanation
(Q)EAA	(Qualified) Electronic Attestation of Attribute
ARF	Architecture and Reference Framework
B2B	Business to Business
B2C2B	Business to Consumer to Business
B2G	Business to Government
BA	Business Area
BRIS	Business Register Interconnection System
BS	Business Scenario
CA	Contracting Authority
CIUS	Core Invoice Usage Specification
DO	Domain Ownership
DNS	Domain Name System
DUNS	Data Universal Numbering System
EC	European Commission
eID	electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
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
EEA	European Economic Area
EN	European Norm
ENISA	European Network and Information Security Agency
EO	Economic Operator
ESPD	European Single Procurement Document
EU	European Union
EUDI	European Digital Identity
EUDIW	European Digital Identity Wallet
EWC	EU Digital Wallet Consortium
GDPR	General Data Protection Regulation
GLN	Global Location Number
GS1	Global Standards 1
IBAN	International Bank Account Number

Co-funded by
the European Union

ID	Identifier
IT	Information Technology
JSON	JavaScript Object Notation
KGV	Konkurransegjennomføringsverktøy
KPI	Key Performance Indicator
KYC	Know Your Customer
KYS	Know Your Supplier
LEI	Legal Entity Identifier
LoA	Level of Assurance
LPID	Legal Person Identification Data
LSP	Large Scale Pilot
M	Month
MS	Member State
NDA	Non-Disclosure Agreement
NIS2	Network & Information Security 2
ODI	Organisational Digital Identity
OOTS	Once-Only Technical System
PID	Person Identification Data
POS	Point of Sale
Q	Quarter
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
REID	Registered Entity Identifier
RTE	Real Time Economy
rQES	Remote Qualified Electronic Signature
SAAS	Software As A Service
SD-JWT	Selective Disclosure for JWTs (JSON Web Tokens)
SDGR	Single Digital Gateway Regulation
SME	Small and Medium-sized Enterprise
SSI	Self-Sovereign Identity
TBC	To Be Confirmed

TBD	To Be Discussed
TOOP	The Once-Only Principle Large Scale Pilot project
TSP	Trust Service Provider
VAT	Value Added Tax
VC	Verifiable Credentials

1 Introduction

D3.5 Business Scenarios Pilot Plans delivered by: WP3 / Task 3.3

Date: 10 June 2024

Type: Document, Report

Classification: Public

Lead beneficiary: UPRC

1.1 Scope and objective of deliverable

The purpose of deliverable D3.5 “Business Scenarios Pilot plans” is to present:

1. **Definition of the business scenarios (BS)** that are going to pilot **the Organisational Digital Identity (ODI) use case** in the four **business areas (BA)** (B2B and B2G) that were identified during the proposal preparation phase and are stated in the Description of Action:
    a. Public Procurement (BA1)
    b. Know Your Supplier (KYS) (BA2)
    c. Domain Registration (BA3)
    d. Business Document Exchange (BA4)

    The business scenarios for piloting ODI include details on user requirements, credentials / data attributes required by relying parties, which are feeding tasks T3.1 Wallet Provisioning and T3.2 PID/ODI and organizational credentials and WP4.
2. **Design and plans of ODI pilot plans** including the assessment of the pilots.

Deliverable D3.5 presents the **documentation** of the result from phase 1 “Eliciting and representing business requirements and service design” and phase 2 “Detailed design of the Business Scenarios to be piloted” of the Pilot Lifecycle, which constitute the content of piloting subtask T3.3.1 Business scenario Pilot Design within the WP3 workplan under task T3.3 Business Scenarios Piloting.

Deliverable D3.5 is a living document that is going to be internally updated during the project duration as long as the pilot plans are evolving. The **updates** will be issued **every quarter** (September 2024, December 2024) and the last update will culminate to deliverable D3.6 including the final pilot results. As the pilot plans evolve, the next versions will track their execution until the end of the project.

1.2 Methodology of work

The methodology used to produce the present deliverable and achieve its outlined objectives followed an iterative approach. It started with business scenario experts describing the business scenarios using a word template for business scenario definition and guidelines provided by the WP3 lead. The piloting participants (EWC beneficiaries and associated partners having declared interest to pilot the ODI use case) were then asked to formulate their piloting plans, by leveraging a structured pilot plan presentation template. Finally, the defined pilot plans underwent rigorous assessment based on qualification criteria such as relevancy to EU and national policies, impact such as market adoption, and implementation feasibility.

For easier reading of the deliverable, it is important to clarify the following:

- The term “**Business Area (BA)**” is used to refer to the *four (4) areas* (B2B and B2G) that were identified during the proposal preparation phase and are stated in the Description of Action for piloting the ODI use case.

Co-funded by the European Union

- The term “**Business Scenario (BS)**” is used to refer to the specific use cases within each BA. It is important to acknowledge that there may be multiple business scenarios within each BA, which serves to illustrate the diverse applications of the ODI across different contexts. This differentiation not only allows for a more accurate understanding of the ODI’s potential usefulness across various B2G and B2B areas, but also streamlines the agile assessment of business scenarios during piloting.

A mapping between Business Areas and actual Business Scenarios and Pilots plans is provided in section 2.2.1.

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

It should also be noted that in most cases EWC have started to use the term legal person wallet and legal person identification data (LPID) instead of organisational wallet and ODI, as the terminology have shifted in the EU eIDAS expert group.

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 pilot lifecycle phases and the qualification criteria employed to assess the pilot plans.
- Chapter 3 presents the methodology of work, including definition of the business scenario in a summarised way including overview, problem statement, goals, actors involved, steps of the business scenario, legal basis, and quality goals.
- Chapter 4 provides the pilot plans established per business scenario including details on participants and ambition KPIs.
- Chapter 5 presents qualification of the pilot use cases according to the Pilot Assessment Criteria.
- Chapter 6 offers an overview of the pilot’s status at M15.
- Chapter 7 presents some final conclusions and reflections on the work done in piloting ODI/Legal Person Identity in EWC during the first part of the project and presented in this document.

Co-funded by
the European Union

2 Methodology and approach

The piloting methodology adopted in EWC for the ODI business scenarios piloting followed the experiences gained from work done in previous LSPs such as PEPPOL[1], e-SENS[2], and TOOP[3]. Best practices were kept, and adjustments were made to fit the specific context of EWC in conjunction with the four ODI business areas and their participants.

The methodological approach is based on the exploratory and agile pilot-lifecycle approach, with an iterative process that ensures conceptual clarity, practical solutions and learning. Each pilot will go through different phases, but multiple iterations within and between the pilots are expected to occur.

EWC requires a precisely defined pilot lifecycle for several critical factors. Firstly, given the multitude of pilots undertaken, having a structured framework ensures consistency and efficiency across all implementations. With pilots progressing at varying speeds, a standardized lifecycle enables adaptation and management of each pilot’s pace effectively. Moreover, it is worth noting that each Business Scenario may involve multiple pilot instances across different countries. Therefore, a well-defined lifecycle makes it possible to monitor the progression thoroughly, from initiation to completion, for each pilot instance. In addition to facilitating the monitoring of pilot progress, a clearly defined lifecycle also ensures that the European Commission and other project stakeholders receive accurate reports.

The work was carried out in Task 3.3 using collaborative tools or online conference facilities and face-to-face meetings when appropriate. Additionally, for each business scenario and pilot, T3.3 lead and co-lead have been monitoring and discussing with the pilot coordinators during regular calls. A f2f meeting took place in January in Stockholm with the coordinators of the pilots, the wallet providers and the WP3 task leads and co-leads where the beneficiaries presented their pilot plans and received feedback.

2.1 Pilot lifecycle

The Pilot lifecycle consists of three piloting phases with five piloting activities, each of which is designed to deliver specific output needed in subsequent phases. The decision was made to utilize an agile approach so the lifecycle should be seen as an iterative process that will evolve over time as the pilot scenarios and technical solutions evolve. The overall process is illustrated in *Figure 1* below.

[1] PEPPOL Deliverable D9.1 PEPPOL Pilot Lifecycle Management Methodology (PPLM)

[2] e-SENS Deliverable D5.2 Pilot Lifecycle Management Methodology and Workflow Support Tools

[3] TOOP Deliverable D3.4 TOOP Pilot Handbook

Co-funded by
the European Union

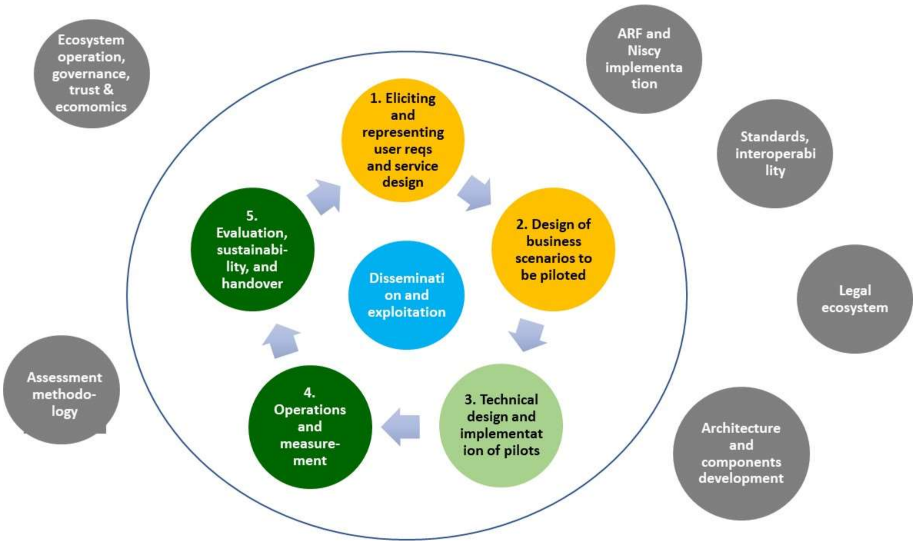
Ecosystem operation, governance, trust & ecomomics
ARF and Niscy implementation
Standards, interoperability
Legal ecosystem
Architecture and components development
Assessment methodology
1. Eliciting and representing user reqs and service design
2. Design of business scenarios to be piloted
3. Technical design and implementation of pilots
4. Operations and measurement
5. Evaluation, sustainability, and handover
Dissemination and exploitation

Figure 1 Pilot lifecycle phases.

The Pilot Design phase (orange circles 1. and 2. in the figure above) includes the elicitation and representation of user requirements and service design. The Pilot Implementation phase (light green circle 3. in the figure above) includes the technical design and implementation of the pilots and the Pilot Running, Evaluation and Handover phase (dark green circles 4. and 5. in the figure above) include the operations and measurement activities and the evaluation of the pilot results, their sustainability, and handover.

During the course of the pilot lifecycle phases and activities, the pilots liaise with a number of activities in the other WPs, namely:

- Architecture and components development (WP4, T3.1, T3.2)
- Standards and interoperability (WP4), ecosystem operation, governance, trust and economics (T4.2)
- ARF and EUDI wallet reference implementation (NiSCY implementation)
- Legal ecosystem
- Assessment methodology
- Dissemination and exploitation strategy

The three piloting phases spread along two EWC piloting subtasks (T3.3.1 and T3.3.2) and five piloting activities that together constitute the piloting work plan of EWC in the following way, as depicted in Table 1.

Table 1 Mapping of piloting phases, activities and EWC piloting sub-tasks

Piloting phases	Pilot Lifecycle activities	EWC subtask
Pilot design	1. Eliciting and representing user requirements and service design	T3.1.1 Business scenario Pilot Design
	2. Design of business scenarios to be piloted	
Pilot Implementation	3. Technical design and implementation of pilots	T3.3.2 Business Scenario Pilot implementation, Running & Evaluation
Pilot Running, Evaluation and Handover	4. Operations and measurement	
	5. Evaluation, sustainability, and handover	

During the Pilot Design phase (activities 1 and 2), pilots are defined, designed, and planned. This includes the following iterative steps for each pilot:

- Detailed descriptions and business flows

Co-funded by the European Union

- Definition of credentials/data attributes that will be required by the verifiers/relying parties, type of source, authentic sources, preferable protocols.
- Extraction of user requirements including issuer, holder and verifier requirements and also non-technical requirements regarding governance, implementation with existing systems, etc.
- Design of the user journey
- Planning of the pilot including assessment of capabilities of existing partners.

The implementation, running (activities 3 and 4) and evaluation (activity 5) pilots are executed.

The execution includes the following iterative steps for each pilot:

- Integration of the specifications, tools and capabilities in the systems of the piloting stakeholders.
- Testing of the pilot solutions, reaching of technical readiness, and installing pilot systems in pre-production environments.
- On-boarding pilot participant organizations and training users, evaluating the pilot, providing feedback and assessing sustainability.

2.2 Business scenario and pilot plans

2.2.1 Identification of pilots

During the proposal preparation phase and accordingly in the Description of Action four ***Business Areas*** *(BAs)* in B2B and B2G were identified for piloting the ODI use case.

In the beginning of the project, interested stakeholders (beneficiaries and associated partners) discussed and defined specific use cases within each BA, the ***Business Scenarios*** *(BS)*. The business scenarios fed with requirements WP4 and tasks T3.1 and T3.2 for wallet provision, definition of legal person wallet, definition of Legal Person Identification Data (LPID) and other organisational credentials required.

Afterwords, stakeholders proposed their pilot plans. Any pilot plan should fall under one of the defined ODI business scenarios and could apply to one or more ODI business scenarios. It is important to mention that we will track the pilots at Pilot Plan level because that is what the Beneficiaries commit to. The table below shows the complete mapping from Business Areas to Business Scenarios and Pilot Plans.

Table 2 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	**P3.1.1** - 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

Co-funded by the European Union

The piloting participants were asked to define the business scenarios and the pilot plans using specific templates. By following the structured templates, pilot participants ensure a comprehensive and systematic approach to outlining the business scenarios and pilot plans, facilitating the planning and evaluation of the pilots. The templates are presented in the sections below.

2.2.2 Business scenario structure and contents

The business scenario template consists of two sections: a summarized presentation of the business scenario one and a detailed description.

The summarized presentation of each business scenario includes the following elements:

- Business scenario overview.
- Problem statement – describes the nature of the problem, stakeholders involved and current volume of service usage.
- Goals of the business scenario.
- Main actors and roles involved.
- Steps of the business scenario.
- Data objects / credentials and authentic sources involved.
- Quality goals and performance indicators / impact statement.
- Legal basis and possible barriers.
- Consortia – which stakeholders (from the consortium and outside the consortium) have interest in this business scenario.

The detailed description includes:

- **Business scenario description:** This section provides an overarching overview of the scenario, detailing its relevance and goals. It includes elements such as the problem statement and objectives related to value, quality, and domain significance.
- **Process description:** Here, the main actors, roles, and steps involved in the scenario are outlined. Additionally, it delineates the flow of events and defines the data objects and authentic sources utilized throughout the process.
- **Architecture and use of building blocks:** This section addresses the use of technologies and building blocks infrastructure established at both EU and Member State level. It highlights the architectural framework supporting the pilot implementation.
- **Implementation and Impact:** Finally, this section evaluates the readiness of participants, identifies potential risks, and assesses the overall feasibility of implementation. It also considers the anticipated impact of the scenario on stakeholders and the broader ecosystem.

2.2.3 Pilot plan structure and contents

Each pilot plan includes the following sections:

- Pilot idea/Hypothesis – what will be piloted within EWC under the specific business areas.
- Pilot values and goals – what is the business usability, the member state usability (for authorities) and what the pilot goals are.
- Pilot description – the pilot is described referring to pre-conditions, steps, interaction and information flow.
- Protocols and infrastructure responsibilities – this part includes the protocols/standards that are intended to be used for issuing/receiving attestations, and also what already exists in terms of infrastructure and what needs still to be done, use of national infrastructure, systems/solutions that are going to be connected.

Co-funded by
the European Union

- Attestations/Attributes – this part should include the list of attestations under the current practice and the ones that are going to be delivered via the wallet.
- Actors and Roles – the organizations involved and their role. It is important to specify whether it is an organization involved in EWC as beneficiary or Associated Partner, or if it is an external party.
- Delimitations
- Implementation and evaluation plan – this part includes some information on steps for implementation including timelines if possible and factors that may influence the execution of the pilot plan.
- Ambition KPIs.

2.3 Qualification criteria

2.3.1 Introduction to criteria needed for assessing pilots

The inclusion of various organizations has been made on the basis of initial piloting intentions which were expressed at the time the EWC consortium was being constructed and the EWC proposal was being formulated. Based on those initial piloting intentions, EWC has defined four business areas (Public procurement, Know your Supplier, Domain holder verification and Business Document Exchange).

During the project, the prospective piloting organizations were expected to formulate detailed pilot plans in order to ensure that piloting will be tangible, valuable and effective. In order to assist the organizations in moving from business scenarios and abstract piloting intentions to specific pilot plans which bring value to the project, some principles and criteria for assessing pilot plans were followed. These principles and criteria provide an objective basis for assessment of WP3 ODI pilots and ensure that key aspects of the EWC approach and of expectations raised on the project by the European Commission are reflected as requirements for suitability and feasibility of any WP3 ODI pilot that proceeds to implementation and execution.

The criteria for piloting assessment for EWC WP3 ODI pilots follow three categories:

- **Relevance** to EU and national policy as well as the Organisational wallet concept according to EWC.
- **Impact potential**, with respect to maturity of processes in scope and relevant stakeholder communities
- **Implementation feasibility**, in terms of realistically achievable goals and relevant conditions that should be in place at European and MS level.

2.3.2 Relevance criteria

There are four criteria in this category:

1. **Relevance to EU legislation / policy**: the pilot will be assessed according to whether it supports existing or upcoming legislative initiatives at EU level (not only the European Digital Identity (EUDI) Regulation 2024/1183[4], but also among others, the Public Procurement

[4] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

Co-funded by
the European Union

Directives 2014/24/EU[5] and 2014/25/EU[6], etc.). It is also important to consider piloting business processes that pave the way to implementation of upcoming EU legislation, such as the Proposal for a Directive to further expand and upgrade the use of digital tools and processes in EU Company Law. When it comes to upcoming legislation at EU level, timing is very important, since the timelines for the adoption and transposition of new legislation should be in line with the timelines of the EWC project so that piloting such use cases can bring concrete value at the appropriate juncture.

2. **Relevance to national policy – MS support for the scenario in the project**: it is important to assess whether the pilot supports any existing or upcoming legislative initiatives at the national level, and whether it overlaps or conflicts with existing or upcoming legislative initiatives at national level.
3. **Relevance to market needs**: this is an important criterion because EWC is interested in pilots where the business process is important for the companies and the market overall. Therefore, it will be assessed whether the business process is recognized as important by the stakeholders concerned.
4. **Cross-border scope**: this is another important criterion to consider, as EWC is focusing in cross-border piloting. Therefore, the pilot will be assessed according to whether there are more than one countries involved, whether the business process is relevant for cross-border intra-community transactions, and whether the pilot is planned to include cross-border transactions.

2.3.3 Impact potential criteria

There are four criteria in this category:

1. **Maturity of the business process**: Priority will be given to pilots where the business process and perhaps also the interoperability requirements have already been addressed at a pan-European, cross-border context. In such cases, which are typical of processes that have an anchor to EU-legislation, EWC will not need to enter a green field where all or most of the work to achieve a sufficiently detailed level of agreed specifications should be done from scratch. In the same way, priority will be given to piloting prospects where there is already prior work that can be leveraged, particularly as a result of previous LSPs or other European initiatives.
2. **Maturity of needed infrastructure**: it is important to assess whether there is a big gap between existing infrastructure and solutions for the pilot actors and the desired future one, whether there is supply of solutions and skills needed (wallets, attestations, interfaces e.g. for relying parties), tight coupling to particular identity registration infrastructures (e.g. EBSI), etc.
3. Links to standardization initiatives: it is important to consider pilots that use standardized building blocks. EWC should avoid non-standardized solutions which will be hard to maintain after the lifetime of the project if no international organization or initiative does not take responsibility for them. When assessing pilot prospects, EWC should seek reassurance that the approach taken is sustainable through existing, or upcoming, pan-European governance for operations and for solutions that are foreseen in the pilot. That said, EWC should be

[5] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance

[6] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC Text with EEA relevance

Co-funded by
the European Union

expected to contribute to the establishment or extension of such structures and procedures in a way that is feasible within the lifetime and resource level of the project.

4. Market adoption potential: this criterion assesses the assurance provided by the pilot that adoption by the intended stakeholder is possible as well as likely. Take-up dimensios related to timing and readiness are considered.

2.3.4 Implementation criteria

There are three criteria in this category:

1. Completeness of scenario / pilot plan description: for a pilot to be approved for going into implementation, the pilot plan should be sufficiently documented in all its aspects and particularly in providing a realistic timeline with milestones as well as a list of expected outcomes. It is important to have a complete business scenario and pilot transaction scenario description with clearly identified pre-conditions which are necessary for the pilot to be successfully initiated and concluded, as well as the post-conditions which are necessary for it to reach full production status.
2. Commitment of participants in all roles foreseen: this criterion assesses whether the proper stakeholders are considered and put in place. This means that the pilot participants at national and, if needed, at European level must be clearly identified and their commitment should be clearly demonstrated. It is important to ensure necessary capabilities for wallets, attestations, relying parties – in the countries where it is needed.
3. Progress against stated goals: this criterion assesses the pilot plan in terms of expected outcomes. Such metrics will help the project monitor pilot execution and determine progress while having the possibility to react in case of adversity and take remedial actions.

2.4 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, it is essential to define distinct pilot states that capture the progression of these initiatives. Each pilot is monitored using the following states:

- **Not started/Commitment to be confirmed:** In this stage, participants may have been contacted and discussions regarding potential implementation scenarios have taken place. While there is interest from involved parties, no formal commitment has been made yet.
- **Committed/ready to start implementation:** In the commitment stage, the pilot has been formally established, with participants committing resources to fulfil their roles and responsibilities. In this stage, there is a clear definition of actions and agreements, as well as outlining of the objectives, timeline, and resources required for successful implementation. Stakeholders onboard and are ready to proceed to pilot execution.
- **In progress:** In the in-progress stage, the technical work for the pilot has been started. Activities such as software development, configuration, deployment, and testing are underway, with people actively working to bring the pilot to fruition. This stage is characterized by ongoing monitoring and project management to ensure smooth progress and addressing of any challenges that may arise.
- **Technical readiness achieved:** Technical readiness of the pilot has been achieved. Signifies the completion of technical work and thorough testing of the environment against stated goals and interoperability criteria established within EWC.

The states described can be summarized in the Table 3 below. The colour-coordination serves to underline how a pilot gets closer to full readiness across its lifecycle.

Co-funded by
the European Union

Table 3 Pilot lifecycle state colour coordination

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

Moreover, in addition to these pilot states, each pilot is also monitored based on two more characteristics:

- **Technical Readiness:** Signifies the completion of technical work and thorough testing of the environment against stated goals and interoperability criteria established within EWC.
- **Business readiness:** Reflects the completion of organizational enablement activities and the beginning of real transactions, indicating the operational readiness of the pilot.

This grading of pilot state is used for reporting the pilot status in section 6.1 of this deliverable.

3 EWC ODI Business scenarios

This chapter presents the definition of **eight (8) business scenarios** EWC WP3 for piloting ODI. Each business scenario begins with an introduction and a problem statement, followed by specific goals. It identifies the main actors involved and outlines the steps of the process, data objects, quality goals, and legal basis. Furthermore, it highlights the stakeholders within the consortium who have an interest in the business scenario.

The chapter presents a rather condensed description of the business scenarios, as these were developed at the end of 2023.

3.1 BS1.1 Public procurement

3.1.1 Introduction

The public procurement business scenario integrates Norway's approach on evidences and Greece's approach on Economic Operator (EO) identification. Public procurement procedures are complicated, multifaceted processes requiring the coordination of several involved actors and the consideration of multiple interoperability layers (legal, organizational, technical, and semantic) while ensuring accountability and transparency. The EC Directives 2014/24/EU[7] and 2014/25/EU[8] aim to reduce administrative burdens and streamline processes for Contracting Authorities (CAs - public agencies) and EOs (companies including SMEs), with the European Single Procurement Document (ESPD) being crucial to this effort. Established by the EC on January 5, 2016, the ESPD[9] simplifies the declaration of financial status and suitability for procurement, sparing businesses from presenting all formal evidence and qualification documents as proof of their compliance with requirements set by the CAs in order to participate in the procurement procedure. The Member State’s CAs are legally bound to recognize the ESPD, enabling companies to easily qualify for any public procurement in Europe, fostering competition, and reducing transaction costs.

In this context, the business scenario intends to demonstrate the use of ODI wallets by EOs for authenticating to a national ESPD service in Greece, enabling their participation in cross-border public procurement procedures. In Norway, the ODI wallet will be used to collect documentation for selection criteria aiming to streamline the presentation of evidence as well as their verification by the CAs.

3.1.2 Problem statement

Manually providing EO, legal representative information, as well as evidence as proof for ESPD selection criteria fulfilment, can be cumbersome. Additionally, CAs face challenges verifying the validity of the provided data, increasing the risk of fraudulent activities.

The current challenges to be addressed with the wallet are the following:

- The manual process is **time-consuming** for economic operators who must repeatedly download new documentation
- **Risk of potential fraud** using PDFs

[7] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance

[8] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC Text with EEA relevance

[9] Commission Implementing Regulation (EU) 2016/7 of 5 January 2016 establishing the standard form for the European Single Procurement Document.

Co-funded by
the European Union

- **Risk of data misinterpretation** by Contracting Authorities, particularly with documentation from other countries
- There is **no standardized method** for sharing documentation across the EU
- **Unnecessary data storage** occurs, as all suppliers download and store large amounts of documentation, much of which is not deleted when outdated.

3.1.3 Goals

The goals of the business scenario are the following:

- **Manual work reduction**: the EO, legal representative details and evidence are now filled in manually.
- **Fraud prevention**: Currently CAs are not able to verify the validity of the EO information.
- **Business growth:** expand business opportunities by making it easier to participate in public procurement procedures.
- **Reduction of administrative burden:** lower administrative burdens on companies and public agencies
- **Security:** EO information is always up-to-date and shared via secure channels

Using wallet technology, Norway's primary functional goal is to simplify the process for any legal entity to collect, use and share continuously authentic and up-to-date credentials and certificates required for their business operations. In Greece, the functional goal is to facilitate the authentication and verification of an EO to an ESPD service by automatically presenting and sharing their LPID information.

3.1.4 Main actors and roles involved

The main actors and roles involved in the business scenario are the following:

- EO: company/legal person who is bidding to a public procurement competition and acts as the wallet holder.
- CA: public agency who is conducting the procurement process.
- Legal representative: natural person who fulfils the ESPD form on behalf of the EO.
- Business Registry: issues a LPID to the EO.
- Wallet provider: issues a legal person wallet to the EO.
- ESPD service/digital tool used for handling public tenders: acts as the relying party.
- Governance entity: entity that governs the procurement process.
- Technological partners: partners who have the technical responsibility of technical solutions used in the business scenario.

3.1.5 Steps / business scenario flow

The business scenario is split between two different flows which are going to be piloted by Norway and Greece respectively:

- Evidence/documentation retrieval and verification (Norway)
- Authentication and verification of EOs (Greece)

3.1.5.1 Evidence retrieval and verification

The steps described below shadow a regular tender and focus on evidence retrieval and verification:

1. A CA creates a tender in KGV (Konkurransegjennomføringsverktøy) which is the digital tool for handling public tenders in Norway and indicates relevant documentation for minimum requirements.

Co-funded by
the European Union

2. EOs reply to the tender in KGV, including a list over requested documentation for minimum requirements. A link in KGV allows them to log in to their wallet. Once logged into the wallet, they can approve that the Verifiable Credentials (VCs) of requested data sources are shared with the wallet of the CA.
3. The EOs hand in their tenders in KGV within given deadline. When opened, the CA will be able to see the VCs of the requested documentation, visualized with green-yellow-red flags. This means they can immediately tell if documentation is valid, if it needs manual control of whether it is invalid. This means more time for evaluating the actual tender, and not controlling the standard minimum requirements.
4. All approvals of sharing VCs are automatically withdrawn after the competition, except of the winning EO's.
5. The VCs of the winning EO will be shared with the CA throughout the contract duration, and a notification will be sent from the wallet to the CA in case the status of the VC changes.

3.1.5.2 EO Authentication and automatic verification of company data

The steps described below focus on authenticating EOs and verifying their company data:

1. EO wishes to generate an ESPD response to participate in a call for tender in a foreign country.
2. EO's legal representative accesses an ESPD service.
3. EO authenticates to ESPD service using their legal person wallet.
4. ESPD service verifies the EO and legal representative identity.
5. EO's legal representative initiates ESPD response generation by importing ESPD request generated by CA.
6. EO's legal representative uses legal person wallet to present company data during the ESPD form response fulfillment.
7. EO's legal representative generates ESPD response (download ESPD XML file).
8. EO submits their bid by including the generated ESPD response.

3.1.6 Data objects / credentials and authentic sources involved

For the evidence retrieval flow, the following authentic sources are involved:

- eBevis: technical solution for sharing qualification data.
- Brønnøysundregistrene: issuer of certification of incorporation (data already defined for eBevis).
- Skatteetaten: issuer of tax certificate (data already defined for eBevis).
- VC-generator: creates the VCs.

For the EO authentication and verification flow the following data objects are involved:

- EO details: company name, address (street, number, postcode, city), country, VAT number, contact details (email, phone number, fax), contact person, website (if applicable).
- Legal representative details: first name, last name, date of birth, place of birth, address, country, contact details (email, telephone), position/acting on behalf of which company.

3.1.7 Quality goals and performance indicators / impact statement

The quality goals are the following:

- User friendly interface for EOs and CAs.
- Operational costs reduction.
- Reduction of time required.
- Trust establishment and security.

Co-funded by
the European Union

- Reduction of administrative burden.
- Increase in cross-border business opportunities.
- Reduction of fraudulent activities.

3.1.8 Legal basis and possible barriers

The business scenario puts in practice the amending eIDAS regulation[10] and holds strong relevance and alignment with EU's established legal framework that governs public procurement, notably the Directive 2014/24/EU[11], and Directive 2014/25/EU[12] alongside the ESPD implementing regulation[13]. The user centric data management introduced by the wallet technology aligns with GDPR[14].

Possible barriers include the technical capacities of Business Registries for issuing LPIDs and the involvement of an external company for creating a wallet. Additionally, resources are needed for developing a GUI and VC-generator.

3.1.9 Consortia

The stakeholders interested in piloting the evidence retrieval flow are the following:

- DFØ
- Brreg (provider of eBevis)
- Brønnøysundregistrene
- Skatteetaten
- iGrant

The stakeholders interested in piloting the EO authentication and verification flow are the following:

- UPRC
- GRNET
- GSIS/MDG
- Telesto

3.2 BS2.1 Know your business partner

3.2.1 Introduction

A business partner is a supplier, partner or any third-party organization outside of the company. If a business partner is not a trusted, verified entity, the company risks financial loss, reputational damage, and exposure to fraud. Sensitive information related to business deals should only be accessible to trusted partners.

[10] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

[11] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance

[12] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC Text with EEA relevance

[13] Commission Implementing Regulation (EU) 2016/7 of 5 January 2016 establishing the standard form for the European Single Procurement Document.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Co-funded by
the European Union

Especially when doing business with companies in other countries, trust, verification of information, security of information handling, obeying laws, and the language barriers complicate cross-border trades.

3.2.2 Problem statement

If a business partner is not a trusted and verified entity, the following problems arise:

- Financial loss
- Fraudulent activity
- Reputation damage
- No traceability of information
- Verification of up-to-date information takes a long time
- Business opportunity loss
- Hindering of cross-border trade

3.2.3 Goals

The goals of the business scenario are the following:

- Increase traceability and security on information handling and data exchange.
- Control of important company information for business since a subset of information can be chosen to pass on and accessible to only few people.
- Diminish fraudulent activities.
- 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.
- Deliver required proofs and certificates in seconds with reduced lead times as a result at a 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. This will probably lead to increased trading cross-borders.

3.2.4 Main actors and roles involved

The main actors and roles involved in the business scenario are the following:

- Legal entity / Business Partner in the role of a wallet Holder and usually also Relying Party
- Legal representatives from legal organizations involved, at least to delegate the rights to request the corresponding attestations to the responsible employees.
- QEAA provider
- Authentic sources (National Business Registry, bank)
- IBAN provider

3.2.5 Steps / business scenario flow

The steps of the scenario are the following:

1. Acquire National Business Registry QEAAs, there will be several QEAAs available.
2. Acquire other EAAs, e.g. IBAN.
3. Exchange organizational attestations including verification.
4. Business partner data transfer to internal IT systems.

3.2.6 Data objects / credentials and authentic sources involved

Some subsets or all of the following information are:

Co-funded by
the European Union

- National Business Registry extract (several QEAAs)
- Other EAAs
- Bank Account (IBAN)

3.2.7 Quality goals and performance indicators / impact statement

The quality goals and expected impact are the following:

- Lower the transaction cost of establishing new relationships and lower the cost of maintaining the information updated.
- Increased trade cross-borders.
- Time to establish business deals (decreased).
- Increased deals with new businesses/ new trusted partners.
- Reduced fraudulent activity.
- Increased satisfaction in trading.
- Reduce cost of data management.

3.2.8 Legal basis and possible barriers

The business scenario is aligned with the revision of Directive 2019/1151/EU[15] on digital tools and process in company law and can be complementary to BRIS[16]. A possible barrier could be that legal person wallets are not yet prioritized by the amending regulation of eIDAS as well as SDGR[17].

3.2.9 Consortia

Stakeholders interested in piloting the business scenario are the following:

- Archipels
- iGrant.io
- Spherity
- INVINET
- UPRC

3.3 BS2.2 Know your customer (KYC)

3.3.1 Introduction

Anti-money laundry laws require that banks know their customers. To open a bank account, a legal person is required to present various documents, many of which are issued by the authorities. Traditionally printed documents are used, but eIDAS legal person wallet enables banks and legal persons to smoothen the process by using electronic attribute attestations instead. A company can use their eIDAS wallet to present the necessary certificates to a bank for opening an account.

[15] Revision of Directive 2019/1151/EU on digital tools and processes in company law

[16] Business Register Interconnection System

[17] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.), vol. 295. 2018

Co-funded by
the European Union

3.3.2 Problem statement

The European Banking Federation estimates that in 2020, approximately 1.5 million bank accounts were opened for companies in Europe. The Anti-Money Laundry laws[18] require that a company presents various certificates to a bank for opening a bank account. In this business scenario, the certificates are issued to the company's eIDAS wallet and then presented to the bank.

The stakeholders involved in opening a bank account are the public authorities issuing the certificates, companies holding them and the banks verifying them.

3.3.3 Goals

The goal is to demonstrate how a company can request the relevant certificates from their domestic authorities in their legal person wallet and present them to a bank for opening an account in a cross-border scenario.

3.3.4 Main actors and roles involved

The main actors and roles involved in the scenario are the following:

- Business registers and tax administrations as issuers
- Company as holder
- Bank as the Relying Party

3.3.5 Steps / business scenario flow

The steps of the scenario are the following:

1. The company receives the relevant electronic attribute attestations from the authorities in their wallet.
2. The company proves the electronic attribute attestations from their wallet to a bank to enable the bank's KYC process.

3.3.6 Data objects / credentials and authentic sources involved

The data objects involved from the business register are:

- Business register extract (EU Company certificate).
- List of beneficial owners (Beneficiary register extract).

The data object from the tax administration is the tax residence certificate.

3.3.7 Quality goals and performance indicators / impact statement

The quality goals are to reduce the manual work and throughput time required in the bank for doing the KYC process for a company. The performance indicator of the goal is the number of certificates that are replaced by electronic attestations of attributes in the process.

3.3.8 Legal basis and possible barriers

The banks' KYC process is mandated by the European anti-money laundry laws (2018/843).

The free movement of capital and services belong to the freedoms of the European single market.

[18] 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)

Co-funded by
the European Union

3.3.9 Consortia

Various business registers have shown interest in the business scenario, including those of Germany and the Netherlands. There are also discussions with banks in Finland, Germany and the Netherlands.

3.4 BS3.1 Domain holder verification by domain registry

3.4.1 Introduction

The newly adopted European Directive NIS 2[19], and specifically article 28, introduced new obligations for domain registries and registrars to have procedures to verify identities of domain holders in article 28. The Directive recommends electronic identity as a solution for this verification, as stated in Recital 111: "*Those procedures should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification*". Furthermore, ENISA's March 2023 publication on domain holder verification[20] highlights eIDAS authentication as a best practice, noting that "*eIDAS is a potential tool for digital identity and should be closely examined for its ability to unify approaches to authentication in the registration ecosystem*."

EUDI Wallet (EUDIW) is a great opportunity to fulfill obligations put of entities in domain registration ecosystem. This scenario describe situation when domain registry wants to verify identity of existing domain holder.

3.4.2 Problem statement

Various cybercrime activities over internet require a working domain name. To register a functional domain name, it was always required to provide personal data of the domain holder. However, the process of verification of the provided data has always been soft and non-binding. This gave cyber criminals big space to hide themselves. Registries and registrars who wanted to address these issues, have always been looking for tools for quick and trustworthy methods of verification of the domain holder.

3.4.3 Goals

The goal is to demonstrate how EUDIW can be used to address requirements of NIS 2 and contribute to fight against cybercrime.

3.4.4 Main actors and roles involved

The main actors and roles involved in the scenario are the following:

- Domain registry as verifier / relying party
- Domain holder as user

3.4.5 Steps / business scenario flow

The steps of the scenario are the following:

1. Domain registry requesting verification sends a link to domain holder pointing to verification website.
2. Domain holder will initialize EUDIW with Person Identification Data (PID).
3. Domain holder will access verification website, scan QR code on the website and approve sharing PID with domain registry.

[19] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)

[20] DNS Identity," ENISA. Accessed: May 31, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/dns-identity

4. Domain registry will match PID with registration data and process request. Registry may store person identifier for subsequent requests of the same person.

3.4.6 Data objects / credentials and authentic sources involved

The data objects used are the PID and LPID.

3.4.7 Quality goals and performance indicators / impact statement

The main quality goal is to increase the number of domains that will go through the domain holder verification processes and save time spent of domain holders in verification processes.

3.4.8 Legal basis and possible barriers

The business scenario is supported by the newly adopted NIS2 Directive.

3.4.9 Consortia

The stakeholders interested in piloting the scenario are the following:

- CZ.NIC
- Internetstiftelsen

3.5 BS3.2 Domain ownership as credential for QWAC issuance

3.5.1 Introduction

Domain ownership (DO) is the information that is held in central registry database and could be potentially queried using services like WHOIS[21]. An entity that wants to present DO can use several techniques to do that. They can either point to a WHOIS service or use DNS service itself either by sending e-mails to contacts related to domain or asking domain owners to publish some records in DNS. These tools can be easily replaced by having DO as credential in the wallet that can be trustfully presented to other party.

One of primary consumers of this information could be QTSPs issuing Qualified Web Authentication Certificates (QWAC). Prior to issuing QWACs, these organizations must verify identity of the requester and domain ownership. For second check they nowadays rely on aforementioned techniques. With DO as credential, they can simplify these two checks into one query to the wallet (PID and DO). This will streamline certificate issuance process which should reduce time for requester.

3.5.2 Problem statement

Domain registry and QTSP issuing QWAC certificate can work together to solve the problem of cumbersome identity and domain ownership checks that are required prior to QWAC issuance.

3.5.3 Goals

The QTSP issuing QWAC will streamline issuance process taking advantage for checking PID and DO EEA via wallets.

3.5.4 Main actors and roles involved

The main actors and roles involved are the following:

- Domain registry as DO EEA issuer.
- QTSP as relying party.

[21] https://who.is/

Co-funded by
the European Union

3.5.5 Steps / business scenario flow

The steps of the business scenario are the following:

1. Domain holder access website with registry portal via EUDIW as authentication method.
2. Domain holder scans QR code on the website and approve sharing it's PID
3. Domain registry will offer to store DO EEA for its domains into the wallet
4. Domain holder will accept, and store DO EEA
5. Domain holder request QTSP for QWAC issuance
6. QTPS requests PID and DO EEA
7. Domain holder approves sharing PID + DO EEA
8. QTPS issues QWAC

3.5.6 Data objects / credentials and authentic sources involved

The data objects and authentic sources involved in the scenario are:

- PID
- Domain registry database as authentic source for DO EEA

3.5.7 Quality goals and performance indicators / impact statement

The main quality goal is to reduce the time spent of the user in a QWAC issuance process. In long term, if these methods become popular, it may reduce cost on QTSP side as, some other methods used for domain ownership checks could be removed.

3.5.8 Legal basis and possible barriers

This procedure may rely on approving standards for QTSPs that QTSPs must follow.

3.5.9 Consortia

The stakeholders interested in piloting the scenario are the following:

- CZ.NIC
- GUNET
- Infocert

3.6 BS4.1 Peppol network registration and use

3.6.1 Introduction

A company, acting as a business partner, registers on the Invinet (B2Brouter) platform. Invinet acts as legal entity and relying party. The company enters its relevant company data, such as the company name, business address and tax number, and then wishes to apply for Peppol access on the Invinet platform. To apply for access, the company must provide a suitable ID assigned to the company that corresponds to a scheme accepted in the Peppol network[22] in accordance with the EAS code list. This can be, for example, a VAT number, an IBAN, a legal entity number or a GLN number. After specifying the company data and requesting Peppol access with a corresponding ID to be used as the Peppol Endpoint ID, Invinet must firstly ensure that the company data is correct and secondly that the ID is assigned to the company. Peppol pursues the "Know your Customer" policy here, which obliges every Peppol service provider to check companies before registering them in the Peppol network.

To avoid fraud and misuse, Invinet must therefore verify the company data for each of its customers before they register on the Peppol network. The complexity of this can arise from the fact that a company can freely decide which ID of the company should be used to register in the Peppol

[22] https://peppol.org/documentation/governance-documentation/internal-regulations-for-use-in-the-peppol-network/

Co-funded by
the European Union

network. For most companies, this is usually the VAT number, but other ID schemes can also be used depending on preference and regulations. Depending on the ID scheme, different documents must be submitted to confirm that the respective ID is assigned to the company. German authorities, for example, must register with the "Leitweg-ID" in the Peppol network. For reasons of simplification, it is initially assumed that the scenario only considers the verification of the VAT number. Other ID schemes can then be added later as required.

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 ID. On the Invinet 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. 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. In a threat scenario, fraudsters could, for example, send fake invoices to companies in the hope that they will be paid by the recipients.

The envisaged process assumes that authenticity proof, the provision of the company's data, as well as the verification of the ID used for registration, can take place directly through the use of the EUDI wallet. The user therefore authenticates himself with his wallet on the Invinet platform and the master data can be automatically transferred to the platform. At the same time, the ID used for authentication is checked with corresponding evidence. After that, Invinet can provide an automated service contract with the corresponding ID and master data for the customer to sign in order to use the Peppol network and potentially other platform services. This automated transfer of data from the company and verification of the data would make it possible to reduce manual effort and increase trust between all parties involved.

3.6.2 Problem statement

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 ID (required due to KYC policy of Peppol). The Invinet platform has 140,000 users, but only a fraction of them is registered for Peppol, as this service requires a special activation. If this service was activated when registering in Invinet via EUDI Wallet, more users would be able to use Peppol directly. On the Invinet side, the registration process 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. 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. In a threat scenario, fraudsters could, for example, send fake invoices to companies in the hope that they will be paid by the recipients.

3.6.3 Goals

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

3.6.4 Main actors and roles involved

The main actors and roles involved are the following:

Co-funded by
the European Union

- Company as a Holder of a Legal Person Wallet
- Invinet as verifier

3.6.5 Steps / business scenario flow

The steps of the scenario are the following:

1. Company wants to register on Invinet and settles username and password
2. Company authenticates with the legal person wallet
3. Invinet verifies authenticity and requests user to adapt company master data from the legal person Wallet.
4. User agrees to use master data on Invinet
5. Either Invinet adapts ID from master data or asks user which ID to use for registration to the Peppol Network.
6. User selects ID.
7. Invinet request corresponding evidence for ID if not yet provided by master data.
8. Invinet receives prove and presents service contract for the user to accept.
9. After accepting the contract, Invinet unlocks the Peppol service for the user.

3.6.6 Data objects / credentials and authentic sources involved

The data objects and authentic sources involved are the following:

- Mandatory Information: Company name, VAT ID, fiscal address, postal code, city, country
- Optional Information: Company Registration Number, IBAN, tax ID, IDs listed in EAS (e.g. DUNS, GLN, LEI, Leitweg-ID, REID, IBAN, CODICE FISCALE, GS1, ...)

The information might be required if a user wants to register for Peppol with a number different from VAT.

Authentic sources could be specific business registries but also financial authorities for tax ID and VAT ID. For other IDs could be banks or other agencies and authorities, depending on the type of ID.

3.6.7 Quality goals and performance indicators / impact statement

The registration process should be as convenient as possible for the user. This should involve as little effort as possible for the Service Provider. At the same time, trust between trading partners on the Invinet platform should be gained as early as possible through registration. As many services as possible should be offered directly to the user. This refers not only to registration and Peppol activation, but also to the trust of IBANs used in Invinet and the activation of other services such as automated tax reporting.

3.6.8 Legal basis and possible barriers

No Barriers currently existing apart from the data protection regulations must be complied with.

3.6.9 Consortia

The stakeholders interested in piloting this scenario are the following:

- OpenPeppol
- Invinet

3.7 BS4.2 Verifiable eReceipt

3.7.1 Introduction

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,

Co-funded by
the European Union

financing, insurance, expense management, etc. The vReceipt business scenario can be broken down into two main usage scenarios:

- vReceipt issuance to a natural person wallet (Usage scenario 1) and
- vReceipt issuance to a legal person wallet when the purchase was made by a natural person (Usage scenario 2).

3.7.2 Introduction

The use of eReceipts 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 eReceipt 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.

3.7.3 Goals

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 business goals are the following:

- Reducing 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.
- Preventing fraud. The receiver of the vReceipt is able to validate that the vReceipt contents haven't been tampered with after it was issued.
- 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 other issuer's properties (such as, legal form and status).
- Issuer's VAT status. To be able to deduct the VAT that the vReceipt contains, the buyer must ensure the seller has a valid VAT number.
- 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.
- Post-sales channel to the buyer. 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.
- Open interoperable ecosystem. Unlike current closed vReceipt 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.

3.7.4 Main actors and roles involved

The main actors and roles involved in the scenario are the following:

- Seller: is the merchant that sells the product and issues the vReceipt pertaining to the product(s) or service(s) sold.
- Buyer: is the person who makes the purchase. In usage scenario 1 they also receive the vReceipt (as a holder) in their wallet and proves it to the receiver.

Co-funded by
the European Union

- Receiver: is the downstream consumer of the vReceipt. Examples of receivers are insurance agencies, financial service providers, accounting firms, etc.
- National business register: issues a PID to the Seller.
- Competent tax administration: issues the Seller a QEAA carrying its VAT number.

3.7.5 Steps / business scenario flow

Two scenarios are supported. In both scenarios, Rami (buyer) is a sales representative of Sales company Ltd and needs to do a business trip to a customer. Rami buys a train ticket from a Train company Ltd. After the trip, Rami needs to claim the travel expenses from his employer.

In Usage Scenario 1, Rami gets the vReceipt in his natural person wallet. The steps are the following:

1. Rami indicates his wallet’s eAddress.
2. Train company’s Point of Sale system hands the receipt contents and Rami's eAddress to the wallet.
3. Train company's wallet issues and sends the vReceipt to Rami’s wallet.
4. Rami presents a proof of the vReceipt to Sales company’s wallet.
5. Sales company’s wallet hands the vReceipt to the expense management/accounting system.

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.

1. Rami indicates Sales company’s eAddress.
2. Train company's Point of Sale system hands the receipt contents and Sales company’s eAddress to the wallet.
3. Train company’s wallet issues and sends the vReceipt directly to Sales company’s legal person wallet.
4. Sales company’s wallet hands the vReceipt to the expense management/ accounting system

3.7.6 Data objects / credentials and authentic sources involved

The data objects and authentic sources involved are the following:

- EAA is a Verifiable eReceipt described using a common data model (e.g. CEN/TS 16931-8:2022). The authentic source involved is the Seller’s Point of sale system / receipt registry.
- EAA: vReceipt issuer’s PID. The source is the national business registry.
- EAA: vReceipt issuer’s VAT number. The source is competent tax administration.

3.7.7 Quality goals and performance indicators / impact statement

- Purchase interaction user experience. Must be easy and fast.
- Speed of purchase interaction. Must have minimal impact on the total purchase activity time.
- Adoption cost for seller. Must not require a completely new system compared with current or near future changes.
- Personal device feature support. Must include support from both iOS + Android.
- Payment method agnostic. Must not be dependent on any one payment method.
- Supports exception flows. Must support also a flow where an erroneous vReceipt is revoked and replaced with a correct one.

3.7.8 Legal basis and possible barriers

There are currently no identified EU laws on vReceipts. A primary challenge is the user experience and device feature support, as slow speed of interaction will not be tolerated in the fast-paced cash registries. A second challenge is the adoption incentives for the sellers. Currently sellers are reluctant to enable sending of receipts to external systems, as they do not see the added value for them.

Co-funded by
the European Union

3.7.9 Consortia

The stakeholders interested in this business scenario are the following:

Within EWC consortium

- Finnish Tax administration
- Finnish Ministry of Finance
- State Treasury Finland
- TietoEVRY
- Findynet
- iGrant.io
- University of Aegean

Outside EWC consortium:

- Multiple members in Finnish eReceipt ecosystem
  - Cash register providers
  - eReceipts operators
  - Accounting and Travel expense management providers
  - Bank and insurance company
- Standardization organizations

3.8 BS4.3 Create a company branch in another country

3.8.1 Introduction

This business scenario is about a company wanting to create a branch in another country than their registered office. This process, as it is today, is very cumbersome since it involves manual controls, there is a lack of standards, it is not very secure, and it does not comply with the proposal for eIDAS 2.0. The goals of this scenario are thus firstly to increase security and technical trust mechanisms for creating a branch, secondly to learn about the techniques and legal challenges for being able to comply with eIDAS 2.0 and thirdly to decrease lead times and manual involvement in the process.

At least the business registries from Norway and Sweden are interested in working together to pilot this business scenario “Create a branch in another country”.

Preconditions to the scenario would be that for example the Norwegian business registry issues a Certificate of Registration to a Norwegian company (or representatives personal) wallet in the form of an attestation.

The main steps in the scenario are that the Norwegian company applies for registering a branch with the Swedish Business registry and in this process the Swedish Business registry accepts the Norwegian Certificate of Registration. This process could also be tested vice-versa in the pilot.

There are many stakeholders who are interested in this scenario. The biggest group of interest would of course be wallet providers and companies using the wallet and the attestations from public agencies such as Business registries in different countries. Other public agencies are also interested in this pilot which would show that the concept works in general and over country borders. Even banks would probably be interested in this scenario.

Disclaimer: The answers in this scenario are tailored to this pilot in accordance with coordination between the Swedish and Norwegian business registry. Whenever technical details are being discussed, the origin is techniques from the Swedish Business registry and processes and technology is probably different in Norway. This will not hinder the execution of this business scenario. This is

Co-funded by
the European Union

also disclaimer that there might be more legal and technical challenges for real-world execution than described here for the pilot.

3.8.2 Problem statement

The challenges that the wallet would fix are the following:

- Paper/Pdf based process
- Long lead times for the end user
- Manual work
- Costly
- Security issue
- No standardized way of doing across the EU/EEA

3.8.3 Goals

The main goal of the business scenario is to achieve a fully digitalized secure process cross border for digital processing in other countries national registers. In addition, achieve the following:

- Short lead time
- Reduce manual work for the users and for the administrative case workers
- Reduce cost for end users and business registries
- A secure process - with verified IDs and documents
- An aligned semantic and communication structures across the EU/EEA

3.8.4 Main actors and roles involved

The main actors and roles involved in the scenario are the following:

- Company representative
- Business registry (for parent company) which acts as Issuer
- Business registry (for registering branch) which acts as Relying Party
- Wallet provider
- IDP

At least Norway and Sweden are interested in acting both as Issuers and Relying party for each other in this scenario.

3.8.5 Steps / business scenario flow

The steps of the scenario as the following:

1. Establish connection between wallet and Relying party (Business Registry)
2. Chose the process of registering a branch in foreign country
3. Provide attestations about parent company and mandate of requester
4. 4 Provide information needed to establish a new branch
5. Sign and submit registration of branch
6. Optional: Pay for registration of branch
7. Optional: Register branch at business register
8. Optional: send attestations of branch to wallet.

Note that the Holder has required and gotten attestations from Issuers beforehand as a pre-condition. The business processes will differ between countries, but the goal is the same

3.8.6 Data objects / credentials and authentic sources involved

The data objects and authentic sources involved are:

Co-funded by
the European Union

- *Parent company information:* Certificate of registration as attestation.
- *Other proofs via other methods, e.g.:* Articles of association, Certificate of Good Standing, Annual account (previous two years), Power of attorney, Copy of passport for non-residents president/vice president.
- *Branch information examples:* name, articles of association, fiscal year, board members, business address.

3.8.7 Quality goals and performance indicators / impact statement

Easier and more secure registration process leads to the following quality goals:

- Shorter time to market for new branch
- Increased customer satisfaction
- Reduced fraudulent activity
- Increased sustainability
- Increased cross border trade
- Increased data quality

3.8.8 Legal basis and possible barriers

The business scenario is aligned with the revision of Directive 2019/1151/EU[23] on digital tools and process in company law. A possible barrier could be that legal person wallets are not yet prioritized by the amending regulation of eIDAS.

3.8.9 Consortia

The following stakeholders are interested in this business scenario:

- Business registers (at least Norway and Sweden)
- Tax agencies (watchers)
- Banks (watchers)
- Wallet provider

[23] Revision of Directive 2019/1151/EU on digital tools and processes in company law

Co-funded by
the European Union

4 EWC ODI Pilot plans

This chapter outlines the **nine (9) pilot plans** the beneficiaries are committed to and according to these pilot plans, the progress will be monitored. It should be mentioned that at the time of preparation of this deliverable, not all pilot plans are very mature, and it is only now that most of the beneficiaries have progress with the discussions on the involvement of necessary actors.

We will monitor the pilot progress along the duration of the project. The sections below present the pilot plan details and the pilot's targeted KPIs.

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

Table 4 and Table 5 below show the pilot plan for the "Issue and verify attestations used as evidence in the procurement process flow (ESPD)" pilot led by DFØ Norway and its targeted KPIs.

Table 4 P1.1.1 – pilot plan overview

BS1.1 Public procurement	
P1.1.1: Issue and verify attestations for evidence in the procurement process (ESPD)	
Pilot idea/hypothesis	Utilize EUDIW for organizations to easily document that they meet the selection criteria in a given public procurement project. 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 like an ISO27001 or tax certificate. 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.
Pilot values and goals	The pilot will implement and evaluate an EUDIW for organizations to show case 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. The goal is to improve public procurement.
Pilot description	The pilot within public procurement will "shadow" an actual procurement process. Based on the ESPD, we will add capabilities to issue and verify attestations on selected data sources that will be used as evidence in the procurement process flow and show how the EUDIW can be used to automate the verification of the evidence throughout the contract period. (eCertis is an EU database mapping selection criteria with evidence in each MS).

Co-funded by
the European Union

Protocols and infrastructure responsibilities	Protocols. Formats and standards: OpenID4VCI, OpenID4VP, W3C, VC/SD-JWT EUDIW infrastructure for piloting. eBevis (national service for public evidence in Norway) eTendering system (probably Artifik) Brønnøysundregistrene (issuing LPID) Cross border will be considered
Attestations and attributes	Attestations (VCs): 1) Company certificate (Breeg) 2) Tax certificate, VAT certificate (Skatt)
Actors & Roles	DFØ governs the procurement process, eForms and ESPD Brreg: Issues legal person identity (ODI), provider of national evidence service (Bevis) Contracting Authority: pilot participant Commercial Business: pilot participant - depends on tender
Delimitations	We assume that the EUDIW infrastructure is in place, ODI is defined and that standards and architecture on issuing and verifying of attributions is in place.
Implementation & Evaluation plan	Local pilot/Proof of Concept in Norway under controlled environment. Can «mock» key components to fast-track PoC.

Table 5 P1.1.1 – KPIs

KPI	Target planned within pilot	Comment
Number of wallet issuing countries	1	Maybe pilot can be extended to the Nordics. In that case 3-4
Number of ODI issuing countries	1	Same as above
QEAA	2	
Number of relying parties	1	Potential in Norway ~2000 (Contracting Authorities)
QTSP providers	1	As first comment
Wallet users (legal persons)	10	2-3000 per year
Wallet users (natural persons)		
Number of transactions completed		10000 per year
Number of qualified signatures issued	10	
Number of ODI credentials shared	10	10000 per year

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

Table 6 and Table 7 below show the pilot plan for the “Automated verification of Economic Operator identity in the procurement process (ESPD)” pilot led by UPRC and its targeted KPIs.

Table 6 P1.1.2 – pilot plan overview

BS1.1 Public Procurement
P1.1.2: Automated verification of Economic Operator identity in the procurement process (ESPD)

Pilot idea/hypothesis	Utilize an EUDIW for organisations to easily authenticate EOs to an ESPD service as part of a procurement process. Scope: showcase how EUDIW can be used by organizations to authenticate themselves to an ESPD service as part of a procurement process. The pilot focuses on streamlining the authentication process to ESPD services and automate the presentation of company data (or legal representative data) which are essential for the efficient fulfilment of the ESPD process.
Pilot values and goals	The pilot will implement and evaluate and EUDIW for organizations to show case the following: 1) How companies or their legal representative authenticate to an ESPD service. 2) How company data can be shared and presented to an ESPD service using the EUDIW. 3) How public contracting authorities can use the EUDIW to verify company data. Pilot goals: 1) 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). 2) Lower administrative burden on companies. 3) Prevent fraud by verifying company identity.
Pilot description	Manually providing EO and legal representative information for ESPD fulfilment can be cumbersome. Additionally, CAs face challenges verifying the validity of the provided data, increasing the risk of fraudulent activities. The pilot will enable the authentication and verification of an EO to an ESPD service by automatically presenting and sharing their company data (LPID information)
Protocols and infrastructure responsibilities	Exchange protocol: OpenID4VC Credential format: JSON SD-JWT The infrastructure to be used is the Greek ESPD Service (Promitheus)
Attestations and attributes	• Authentication: PID, LPID • EO details: company name, address, country, VAT number, contact details, contact person, website (if applicable) • Legal representative details: first name, last name, date of birth, place of birth, address (street, number, postcode and city), country, contact details (email, telephone), position/acting on behalf of which company
Actors & Roles	GSIS/MDG governs the procurement process. UPRC: Technological partner - developer of ESPD service TELESTO: technological partner GRNET: wallet provider GEMI: issues LPID – not within the consortium yet, in discussion Contracting Authority: pilot participant Commercial Business: pilot participant
Delimitations	We assume that the EUDIW infrastructure is in place, and that standards and architecture on issuing and verifying of attributions is in place.
Implementation & Evaluation plan	Design phase

Table 7 P1.1.2 – KPIs

KPI	Target planned	Comment

Co-funded by the European Union

	within pilot	
Number of wallet issuing countries	2	Maybe Norway can participate in the cross-border pilot
Number of ODI issuing countries	2	Same as above
QEAA	2	
Number of relying parties	1	Potential in Greece – around 2000 CAs
QTSP providers	1	
Wallet users (legal persons)	3	
Wallet users (natural persons)		
Number of transactions completed		
Number of qualified signatures issued		
Number of ODI credentials shared	3	

4.3 P2.1.1 Onboarding new Business Partner

Table 8 and Table 9 below show the pilot plan for the “Onboarding new business partner” pilot led by Archipels and its targeted KPIs.

Table 8 P2.1.1 – pilot plan overview

BS2.1 Know your business partner	
P2.1.1: Onboarding new business partner	
Pilot idea/hypothesis	Hypothesis 1: The 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 source through the wallet • A Legal Person wallet can request to another wallet to present attestations (ODI credentials) • A Legal Person wallet can present attestations to a relying party • A Legal Person wallet can “transfer” attestations to an internal system This will be tested initially between an enterprise with its suppliers within its own country and then perform a cross-border exchange of attestations between two European organizations enrolled within the help of business registries from EWC Hypothesis 2: The Legal Person wallet can be used for signature of legal documents and initiate payment leveraging such functionalities from third party applications for signature and payment. The org wallet will ensure the authentication to those applications. Combined hypothesis will enable a company X to onboard a partner Y from signing a NDA, then a commercial contract at an advanced level of assurance and share ODI credentials to verify its legal identity attributes and be able to initiate payment on any product/services trade via the wallet.

Co-funded by
the European Union

Pilot values and goals	This pilot is important to EWC because it is a basic B2B use case with an exchange of documents between 2 companies. It needs ODI wallet functionalities such as wallet to wallet connection, QEAAs presentation and verification, potentially EAAs too. Pilot goals: 1)Prioritized: verify the hypothesis #1 and prove the value to companies to adopt the wallet, reduce the friction in onboarding new partners, reduce fraud and maintain compliance at national and cross border level. 2) Optional: verify hypothesis #2 Keep the pilot as production-ready as possible. Need to validate our capacity to deliver "SCA" in the wallet, have a level high of person identity verification within the wallet (?) and connect with payment providers within EWC
Pilot description	Pilot description in phase 1: 1) Wallet & ODI attestation issuing via business registries 2) Manage attestations request/presentation via qualified employees
Protocols and infrastructure responsibilities	Exchange protocol: Didcomm (available) + OpenID4VCI and OpenID4VP (Q3) Credential Formats: Anoncred + JSON + (SD-)JWT (selective disclosure in Q4) Trust node: Archipels – Ethereum based (+ possibility to test interoperability with another blockchain if crossborder pilot – for example ID Union (GER) and EBSI (SW . GR) Infogreffe will deliver the ODI and QEAAs (legal representative, KBIS or EU company certificate, beneficial owners) Other Business registries will be needed to test cross-border exchange of attestations. Archipels will onboard willing QTSP such as open banking aggregator to issue IBAN attestation for example, in case of missing issuers, Archipels will issue (Q)EAAs from authentic sources. Organisation Wallet(s) for piloting: Archipels (+ possibility to test interoperability with another wallet if cross-border pilot)
Attestations and attributes	**Phase 1 Q1 2024** legal representative, KBIS or EU company certificate, beneficiary owners. **Phase 2** IBAN, Self-declaration attestations signed. **Phase 3** Other attestations to be defined with relying parties to support piloting requirements.
Actors & Roles	Infogreffe Powens/ Tink / Wordline ID NOW/ID360: Authentic source, QSTP, RIVP (inside Archipels wallet) Archipels: Wallet provider/Trust list provider TBC: wallet holder/relying parties/QES provider
Delimitations	**PID availability:** MS PID providers (French State for example) won't deliver PID in time for our pilot starting S1 2024. French PID will only be delivered to the French public EUDIW and not usable for private purpose in the initial phase. Expected collaboration w/ Potential consortium on S2 2024. **Approach selected:** Archipels will provide an ID verification (PVID) that can temporary replace the French PID. S2 2024 Archipels will work on the portability of the French PID delivered by the State
Implementation & Evaluation plan	PHASE 1: National pilot First implementation plan Q1: Selection of the Organization + Design of the pilot Q2: Legal person wallet development and pilot implementation First evaluation plan Q3-Q3: End user testing and evaluation

Co-funded by
the European Union

	Challenges/Risks/Overall feasibility: Interoperability, Trust registries PHASE 2: Cross-border pilot S2 2024 to S2 2025 • Option 1: Archipels wallet and Archipels Trust Registry: This option tests interoperability on a business level (org wallet attestation exchanges, attestation schemas, ...), with only one wallet and TR technology • Option 2: National wallet and Archipels Trust Registry: Archipels offers to provide the infrastructure registration system to another organisational wallet provider. This option tests wallet interoperability • Option 3: Foreign wallet and TR: This option allows to test full interoperability between wallets and TR

Table 9 P2.1.1 – KPIs

KPI	Target planned within pilot	Comment
Number of wallet issuing countries	1 (FR)	Potentially more if business registries require a local org wallet
Number of ODI issuing countries	2	We aim to pilot with Sweden, Germany, the Netherlands, and Greece
QEAA	3 to 4	Kbis, RBE, legal representatives IBAN
Number of relying parties	7+	Recruitment with Infogreffe in Q1 2024
QTSP providers	3	
Wallet users (legal persons)	30+	
Wallet users (natural persons)	30+	
Number of transactions completed	TBC	
Number of qualified signatures issued	TBC	
Number of ODI credentials shared	100+	

4.4 P2.2.1 Open a bank account for a business

Table 10 and **Fel! Hittar inte referenskälla.** below show the pilot plan for the “Open a bank account for a business” pilot led by the Finish Tax Administration and its targeted KPIs.

Table 10 P2.2.1 – pilot plan overview

BS2.2 Know your customer	
P2.2.1: Open a bank account for a business	
Pilot idea/hypothesis	Using an EUDIW for organizations to open bank account cross-border remotely.
Pilot values and goals	The pilot's goal is to reduce fraud and cut costs for financial institution's regulated KYC processes. Pilot values: 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
Pilot description	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).

Protocols and infrastructure responsibilities	Protocols: OID4VP Infrastructure: The Finnish team has deployed a test bank for a national KYC experiment in the Mini-Suomi sandbox.
Attestations and attributes	LPID (if available) Business register extract (EU company certificate) Beneficiary register extract.
Actors & Roles	Finnish tax administration: Issuer of the attestations (synthetic data), company wallets (in sandbox environment), test Relying party German Bundesanzeiger: Issuer of the attestations Spherity: company wallets The Netherlands: KVK (issuer of attestations) Digidentity: company wallets Also discussions with banks for a potential relying party role in the pilot.
Delimitations	The pilot is limited to using synthetic data on fictional companies.
Implementation & Evaluation plan	The goal is to finish the first phase of the pilot in September 2024.

Table 11 P2.2.1 – KPIs

KPI	Target planned within pilot	Comment
Number of wallet issuing countries	3	DE, NL, FI
Number of ODI issuing countries		
QEAA	0	No QTSP audit possible in project timeframe
Number of relying parties	3	One bank in each country
QTSP providers	0	No QTSP audit possible in project timeframe
Wallet users (legal persons)	15	Assumption that 5 company representatives will be attracted from each country to give it a try
Wallet users (natural persons)	0	No natural person wallet in the pilot
Number of transactions completed	45	5 companies in 3 countries, each makes 3 transactions 5x3x3=45
Number of qualified signatures issued	0	No signatures/seals in the pilot
Number of ODI credentials shared	2	EU company certificate/UBO

4.5 P3.1.1 Domain holder verification by domain registry

Table 12 and Table 13 below show the pilot plan for the “Domain holder verification by domain registry” pilot led by CZ.NIC and its targeted KPIs.

Table 12 P3.1.1 – pilot plan overview

BS3.1 Domain holder verification by domain registry	
P3.1.1 Domain holder verification by domain registry	
Pilot idea/hypothesis	Using an EUDIW for organizations to verify identity of domain holder. Recently approved NIS2 legislation implies requirement on domain registries and registrars to put more effort to verify identity of domain holder and these organizations are seeking for tool how to do this. NIS2 recital mentions that eID should be considered for these goals. EUDIW is ideal tool how to achieve this. Domain holder usually goes first to domain registrar where he fills his information, and this information is transferred via registrar-to-registry protocol (EPP) from domain registrar to domain registry. At the moment, there is no unified agreement if this verification will be done by registry or registrar. Two scenarios should be considered that this identity check will be done at the registry and registrar.

Co-funded by the European Union

Pilot values and goals	The pilot's goal is to fulfill obligations put on entities in the domain registration ecosystem and comply with EU legislation.
Pilot description	Domain holders are both natural and legal persons. Through the EUDIW they need to present information that will allow to match identity with information stored in registry. The steps of the flow are the following: 1. Domain registry requesting verification sends a link to domain holder pointing to verification website 2. Domain holder will initialize EUDIW with PID 3. Domain holder will access verification website, scan QR code on the website and approve sharing PID with domain registry 4. Domain registry will match PID with registration data and process request. Registry may store PersonIdentifier for subsequent requests of the same person.
Protocols and infrastructure responsibilities	Protocols for online flow (OID4VP, SD-JWT) and protocols for registry to registrar communication (EPP) will be used. Infrastructure: Registry infrastructure, Registrant portal, Verification portal, Registrar infrastructure, Registrar portal
Attestations and attributes	PID/LegalPID of legal and natural person
Actors & Roles	CZ.NIC as relying party Internetstiftlesen (.SE) as relying party. The following partners are under question: DENIC (.DE), CIRA (.CA). EIF (.EE)?
Delimitations	There is no registrar in the consortium. It is not clear whether the PID can be shared between several parties. Not clear who can act on behalf of the organization.
Implementation & Evaluation plan	By the end of 2024 verification portal for .CZ will allow to use EUDIW for domain verification, at the beginning 2025 all wallets in consortia will be invited to test with our relying party.

Table 13 P3.1.1 – KPIs

KPI	Target planned within pilot	Comment
Number of wallet issuing countries	1	CZ (any other may follow)
Number of ODI issuing countries	1	Any ODI country may participate
QEAA	0	Only PID/LPID is assumed
Number of relying parties	1	CZ.NIC verification portal
QTSP providers	0	
Wallet users (legal persons)	10+	Organizations in consortia will be asked to participate
Wallet users (natural persons)	20+	Colleagues in CZ.NIC will be asked to participate
Number of transactions completed	30	Each user will add one transaction
Number of qualified signatures issued	0	
Number of ODI credentials shared	10+	

4.6 P3.2.1 Domain ownership as credential for QWAC issuance

Table 14 and Table 15 below show the pilot plan for the “Domain ownership as credential for QWAC issuance” pilot led by CZ.NIC and its targeted KPIs.

Co-funded by the European Union

Table 14 P3.2.1 – Pilot plan overview

BS3.2 Domain ownership as credential for QWAC issuance	
P3.2.1: Domain ownership as credential for QWAC issuance	
Pilot idea/hypothesis	Using an EUDIW for organizations to request QWAC issuance. QWACs are issued by QTSPs after strong identity verification and domain ownership check. Domain ownership check is traditionally done via sending a confirmation link to the emails under the domain or requesting including a code in DNS. This domain ownership check can be replaced by checking VC confirming domain ownership and issued by domain registry.
Pilot values and goals	Domain registry and QTSP issuing QWAC certificate can work together to solve the problem of cumbersome identity and domain ownership checks that are required prior to QWAC issuance.
Pilot description	The steps describing the flow are the following: 1. Domain holder access website with registry portal via EUDIW as authentication method. 2. Domain holder scans QR code on the website and approve sharing it's PID 4. Domain registry will offer to store DO EEA for its domains into the wallet 5. Domain holder will accept, and store DO EEA 6. Domain holder request QTSP for QWAC issuance 7. QTPS requests PID + DO EEA 8. Domain holder approves sharing PID + DO EEA 9. QTPS issues QWAC
Protocols and infrastructure responsibilities	Protocols: standard protocols used during QWAC issuance. Domain registry infrastructure and QSTP infrastructure
Attestations and attributes	PID and new credential about domain ownership (DO)
Actors & Roles	CZ.NIC as EAA issuer Infocert (GUNet) as relying party
Delimitations	Domain verification procedures are part of QTSP accreditation and are not easy to change.
Implementation & Evaluation plan	Q4 2024 – Login to registrant portal will be implemented in CZ.NIC Q1 2025 – Issuing of Domain Ownership credential in registrant portal will be implemented in CZ.NIC.

Table 15 P3.2.1 – KPIs

KPI	Target planned within pilot	Comment
Number of wallet issuing countries	1	CZ (any other may follow)
Number of ODI issuing countries	1	Any ODI country may participate
QEAA	0	Only PID/LPID is assumed, DO credential will be EAA
Number of relying parties	2	CZ.NIC registrants portal, QTSP (I.e Infocert)
QTSP providers	1	
Wallet users (legal persons)	10+	Organizations in consortia will be asked to participate
Wallet users (natural persons)	20+	Colleagues in CZ.NIC will be asked to participate
Number of transactions completed	30	Each user will add one transaction
Number of qualified signatures issued	0	

Co-funded by the European Union

Number of ODI credentials shared	10+	

4.7 P4.1.1 Peppol network registration and use

Table 16 and Table 17 below show the pilot plan for the “Peppol network registration and use” pilot led by Invinet/OpenPeppol and its targeted KPIs.

Table 16 P4.1.1 – pilot plan overview

BS4.1 Peppol network registration and use	
P4.1.1: Peppol network registration and use	
Pilot idea/hypothesis	Using an EUDIW for organisations by the end-users (public and private organisations that want to use the Peppol network to send and receive standard format business documents, such as purchase orders, invoices, requests for payment) to register with the Service Providers of the Peppol network and the distributed capability register consisting of SML and SMPs, to easily identify themselves. Scope includes the exchange of standardized business documents, such as purchase orders, invoices, and requests for payment, primarily via the Peppol network. Peppol (https://peppol.org/) enables public and private organizations to send and receive standard format business documents in an open and secure network through the use of Peppol-accredited Service Providers and supported by scalable governance and agreement framework. Once connected to the Peppol network (via a Peppol Access Point – AP), public agencies and private enterprises can quickly and easily reach any other trading partner using Peppol, hence creating the foundation for a continuously evolving ecosystem for exchanging and exploiting the value created when exchanging structured data.
Pilot values and goals	The pilot will implement and evaluate and EUDIW for organizations to show case the following: 1) How end-users can be registered with the Service Providers of the Peppol network. 2) How end-users can be identified and can be identifiable either directly from the end user or via the service providers. 3) How can end-users be verified as trusted receivers in the Peppol network The main goal is to make Peppol network registration and use better, faster, more reliable
Pilot description	The pilot aims to use ODI and legal person wallet for the registration of the end users and to make the end users of the network identified and identifiable either directly from the end user or via the service providers. This will enable registration and trusted verification of the end-users who act as receivers in the Peppol network. Currently, the Peppol network has 600.000 end-users (companies) as receivers.
Protocols and infrastructure responsibilities	Infrastructure: EUDIW infrastructure for piloting Invinet service provider End-users of Invinet Business registries (issuing LPID) Cross border is guaranteed across the EU and beyond. Peppol is present in all EU countries and in 41 countries globally, connecting thousands of SME’s, businesses, and public organizations.
Attestations and attributes	Attestations: • Company certificate (business registries)

Co-funded by the European Union

	- More to be defined based on the internal regulations of Peppol (chapter 3 of the entity identification policy) Mandatory Information: Company name, VAT ID, Fiscal address, Postal code, City, Country Optional Information (for next phase): Company Registration Number, Tax ID, IDs listed in EAS (e.g. DUNS, GLN, LEI, Leitweg-ID, REID, IBAN, CODICE FISCALE, GS1, ...) The information might be required if a user wants to register for Peppol with a Number different from VAT
Actors & Roles	OpenPeppol as entity that governs the Peppol network Invinet as relying party (Peppol Service Provider) DFO as credential issuer (Peppol Authority) Telesto as technology partner UPRC as technology partner
Delimitations	We assume that the EUDIW infrastructure is in place, and that standards and architecture on issuing and verifying of attestations is in place.
Implementation & Evaluation plan	Proof of Concept with Invinet under controlled environment

Table 17 P4.1.1 – KPIs

KPI	Target planned within pilot	Comment
Number of wallet issuing countries	5* TBC	
Number of ODI issuing countries	5* TBC	
QEAA		
Number of relying parties	1	All the Peppol Service Providers
QTSP providers		
Wallet users (legal persons)	5* TBC	840000 end users of Peppol
Wallet users (natural persons)		
Number of transactions completed		
Number of qualified signatures issued		
Number of ODI credentials shared		

4.8 P4.2.1 Verifiable eReceipt

Table 18 and Table 19 below show the pilot plan for the “Verifiable eReceipt” pilot led by the Finish Tax Administration and its targeted KPIs.

Table 18 P4.2.1 – pilot plan overview

BS4.2 Verifiable eReceipt	
P4.2.1: Verifiable eReceipt	
Pilot idea/hypothesis	Using an EUDIW for organizations to issue, hold and rely on verifiable eReceipts (vReceipt) as an electronic attestation of attributes. A seller (of a travel ticket, parking fee, hotel accommodation) issues a vReceipt, together with business & VAT proofs. The buyer (or their employer) holds the vReceipt. The buyer passes the vReceipt to their employer for travel expense/cost management and accounting. Digitalization of receipts and automation of accounting are key components of Real Time Economy.

	Manual processing of receipts by employees, managers and accountants creates significant costs in societal scale (esp. in B2B/B2C2B). Interoperable exchange and automated processing of digital receipts are surprisingly challenging to execute in large scale. The Real Time Economy (RTE) program led by Finnish State Treasury orchestrates ecosystem & develops Verifiable eReceipt specifications in Finland.
Pilot values and goals	Pilot goals: 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. A person can request automatic delivery to an employer system (e.g. expense management) *Additional goals* Efficient negotiation method Compound proofs (or other method of proving VAT through vReceipt) Archival of proofs (self-contained proving Pilot values: Structured vReceipt supports the receiver in automating their cost management and financial reporting processes. The vReceipt helps the receiver to validate the seller’s identity and VAT status. The vReceipt’s digital signature prevents fraud. Automation saves the buyer’s time when making expense reimbursements. Negotiation increases interoperability and makes adoption easier for sellers. Verification of archived receipts impact auditing costs and prevent fraud.
Pilot description	Scenario 1 - Seller issues the vReceipt to the buyer’s natural person wallet and the buyer presents it to their employer: 1. Rami buys a ferry ticket. 2. Rami and the seller’s system negotiate the delivery / connection details 3. Ferry company’s PoS system hands the receipt contents and delivery to the wallet 4. Ferry company's wallet issues and sends the vReceipt to Rami’s wallet using the negotiated protocol 5. Rami presents a proof of the vReceipt to employer’s wallet (employer system) 6. Employer’s wallet hands the vReceipt proof to the expense management/accounting system 7. Accounting archives the vReceipt 8. Tax auditor verifies the vReceipt years later in tax audit Scenario 2 - Seller issues the vReceipt directly to the legal person wallet of the buyer’s employer 1. Employer authorizes Rami to negotiate delivery of attestations 2. Rami buys a ferry ticket. 3. Rami negotiates delivery directly to employer’s wallet. 4. Ferry company's Point of Sale system hands the receipt contents and delivery details to the wallet 5. Ferry company’s wallet issues and sends the vReceipt directly to Employer’s wallet 6. Employer’s wallet hands the vReceipt to the accounting system 7. Accounting archives the vReceipt 8. Tax auditor verifies the vReceipt years later in tax audit
Protocols and infrastructure responsibilities	Protocols and standards: OID4VC + SD-JWT (Aries stack available as well) CEN/TS 16931-8:2022 (eReceipt data model) Engagement protocol A first draft of Engagement Protocol has been cretaed – a technical specification for negotiating delivery, connection and business context details.

	Infrastructure: MiniSuomi infrastructure and pilot partner systems
Attestations and attributes	1. Verifiable eReceipt As per CEN/TS 16931-8:2022 Issuer: merchants 2. vReceipt issuer's PID Carries the name and identifier of the merchant Issuer: national business register Potentially attached to or provided in conjunction with the vReceipt 3. vReceipt issuer's VAT number Carries the VAT number of the seller, to enable the buyer to ensure VAT deduction right Issuer: national tax authorities Potentially attached to or provided in conjunction with the vReceipt
Actors & Roles	Finish tax administration office as LPID provider Finish tax administration as VAT number issuer Finnish state treasury as employer/receiver University of Aegean/Fast Ferries as issuer of vReceipt.
Delimitations	The vReceipts will be issued, held and verified in test environments and will be synthetic / test data
Implementation & Evaluation plan	The pilot will be implemented by the end of 2024

Table 19 P4.2.1 – KPIs

KPI	Target planned within pilot	Comment
Number of wallet issuing countries	3	We can use natural person wallets from: SE (iGrant.io), Germany (Lissi), Spain (validatedID)
Number of ODI issuing countries	0	No ODI credentials in this pilot.
QEAA	0	No QEAA issued in this pilot
Number of relying parties	1	We are studying interested parties to consume vReceipts (e.g. Amadeus, travellers' employers)
QTSP providers	0	No QTSPs in this pilot
Wallet users (legal persons)	0	We assume vReceipts are issued primarily to the wallets of natural persons (travellers)
Wallet users (natural persons)	100	We assume holders of vReceipts are mostly "Friends and family"
Number of transactions completed	100	We assume holders of vReceipts are mostly "Friends and family"
Number of qualified signatures issued	0	No QES in this pilot
Number of ODI credentials shared	0	No ODI credentials in this pilot.

4.9 P4.3.1 Create a company branch in another country

Table 20 and Table 21 below show the pilot plan for the "Create a company branch in another country" pilot led by Bolagsverket Sweden and its targeted KPIs.

Co-funded by the European Union

Table 20 P4.3.1 – pilot plan overview

BS4.3 Create a company branch in another country	
P4.3.1: Create a company branch in another country	
Pilot idea/hypothesis	Hypothesis 1: The EUDIW can be used in the process for creating a branch in another country in a user friendly way 1) The wallet can be used for authentication 2) The wallet can be used for signing 3) The wallet can present attestations to a relying party 4) The wallet can be used for payment Hypothesis 2: The EUDIW for a RP can be used for accepting presented attestations and use them in internal business processes.
Pilot values and goals	Pilot goals: *Prioritized*: verify the hypothesis 1 (statement 1-3) and hypothesis 2 *Optional*: verify hypothesis #1 (statement 4 payment) Keep the pilot as production-like as possible This pilot is important to EWC because it has focus on all functionality of a ODI wallet; authentication, signatures (rQES), acceptance and verification of attestations, and possibly payments.
Pilot description	Pre-conditions: The wallets have valid PIDs: that can be verified The Holder has required and gotten attestations from Issuers beforehand There is a non-mobile format wallets which organizations can use Steps for the pilot: 1. Establish connection between wallet and Relying party (Business Registry) 2. Chose the process of registering a branch in foreign country 3. Provide attestations about parent company and mandate of requester 4 Provide information needed to establish a new branch 5. Sign and submit registration of branch 6. Optional: Pay for registration of branch 7. Optional: Register branch at business register 8. Optional: send attestations of branch to wallet. Disclaimer: Business processes will differ between countries, but the goal is the same
Protocols and infrastructure responsibilities	Protocols: Attestation exchange protocol: OIDC4VP (as pointed out in the ARF) Credential Formats: JSON + (SD-)JWT Trust node: EBSI HAIP All piloting Business Registers will implement complete functionality: EU Company Certificate (QEAA) requesting and issuing (incl. LPID as described in separate pilot) Business Register Wallet implementation New register for QEAAs New login functionality Bolagsverket will take lead for creating a schema for the LPID and EU Company Certificate Legal Person Wallet(s) for piloting: TBD Everyone will use the same trust lists

Co-funded by
the European Union

Attestations and attributes	EU Company Certificate (QEAA) containing (a) the name of the company. (b)the legal form of the company. (c)the registration number of the company and the Member State where the company is registered. (d)the EUID of the company. (e)the registered office of the company. (f)the postal or contact address of the company. (g)the electronic address of the company. (h)the date of registration of the company. (i)the amount of the capital subscribed. (j)the status of the company. (k)the particulars of any persons who either as a body or as members of any such body are authorised by the company to represent it with respect to third parties and in legal proceedings and whether those persons may do so alone or are required to act jointly. (l)the object of the company. (m)the duration of the company. (n)details of the company website where such details are recorded in the national register. If time permits, we could also implement other QEAAs: such as Power of Attorneys, Signatories and Beneficial Owners which are also used in this process. Branch evidence will be given directly in the business registers eService.
Actors & Roles	Business Registers: Bolagsverket (SE), Brønnøysundsregistrene (NO), PRH (/Vero?) (FI) as Authentic source, relying party, QEAA provider, legal person wallet holder EBSI: Trusted list provider
Delimitations	The proposed schema will be usable for the pilot, but might need refining after the pilot before production use. We will only implement basic functionality in the wallet application. Not all Business register internal processes will be adapted to the pilot
Implementation & Evaluation plan	First implementation plan Q1 + Q2: Implementing creation of LPID Q3 + Q4: Design and implementation of this pilot First evaluation plan Q4+Q1 2025: Evaluation of this pilot, incl. end-user testing

Table 21 P4.3.1 – KPIs

KPI	Target planned within pilot	Comment
Number of wallet issuing countries		
Number of ODI issuing countries	X	Executed in the LPID issuing pilot
QEAA	X	
Number of relying parties	X	
QTSP providers		
Wallet users (legal persons)	X	

Co-funded by
the European Union

Wallet users (natural persons)	X	
Number of transactions completed	X	
Number of qualified signatures issued		
Number of ODI credentials shared	X	

5 Assessment of pilot plans

This chapter includes the qualification of all pilot plans as agreed within the EWC consortium. The assessment was done according to the criteria presented in section 2.3 of this deliverable.

The qualification uses the color-coding presented in the following table.

Table 22 Color-coding of pilot qualification

🟩	High value/potential/feasibility, low risk
🟩	Good value/potential/feasibility, some risk with unresolved issues
🟨	Evidence of value/potential/feasibility, many issues unclear, medium or unknown risks
🟧	Indications of critical inhibitors and increased risk factors
🟥	Showstoppers evident
⬜	Not in scope

There is one qualification sheet per each pilot plan, where the assessment is made first on the suitability applying the criteria and then on the level of risk associated with not meeting the stated intentions and the suitability potential.

The following sub-chapters present each pilot plan qualification sheet.

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

CRITERIA		Assessment for suitability and feasibility	Risk analysis
1	**Relevance**		
1.1	**Relevance to EU/domain legislation/policy**	Strong relevance and alignment with the European Union's established legal framework that governs public procurement, notably Directive 2014/24/EU, Directive 2014/25/EU and Directive 2014/23/EU alongside the ESPD. These directives aim to enhance the procurement processes through simplified procedures, while combating corruption and fraud. Advancements such as eIDAS 2.0 and the utilization of digital wallets facilitate the provision of evidence from trusted sources, thereby reinforcing trust and automation in procurement transactions. However, the approach of the pilot on the evidence semantics overhauls the mappings that have been done over the years around eCertis. The pilot offers a new way to provide evidences, which is bypassing the current legal arrangements in the EU, but it is worth the effort in order to show a potential new way	High risk There is a notable potential overlap, and even conflict with the OOTS. There is fundamental conceptual misalignment between the OOTS approach of evidence retrieval and the user centric approach in evidence retrieval through digital wallets and Self-Sovereign Identity (SSI) techniques. However, leveraging SSI techniques and offering alternative ways for evidence retrieval holds promise in bridging existing gaps in OOTS and complementing it. The pilot will need new legal arrangements in order to go into mass scale production.

		forward in a domain where interoperability is stalled for years.	
1.2	**Relevance to national policy and MS support**	Strong relevance to the "Norwegian Model" (Norgesmodellen) which focuses on requirements to be governed throughout the contract period. The pilot will showcase how this can be achieved in an efficient way using the wallet. It will also act as potential input to the ongoing work of renewing the national public procurement legislation.	Low risk In Norway, the stakeholders are aligned and there can be acceptance, even though the legal challenges may remain.
1.3	**Relevance to market needs**	Strong alignment with market needs, specifically in addressing the simplification of public procurement processes, a need that has been extensively studied and highlighted in recent years. (Single Digital Market) Despite the risks, the pilot gives an opportunity to the market to simplify the procedures and enhance digitalization.	Low risk in the Norwegian, and maybe Nordic, context.
1.4	**Cross-border scope**	The pilot can examine potential cross-border scenarios and synergies in which a Norwegian company uses a wallet to share evidence to the Greek ESPD service	Medium risk It remains a question whether other countries will try the new Norwegian approach on evidences.
2	**IMPACT**		
2.1	**Maturity of business process and infrastructure**	The business process is mature, well researched and documented. Prior work serves as a robust foundation for further development and expansion (PEPPOL, e-SENS, TOOP). The evolution of eProcurement can be influenced through the interconnection of eForms, eCertis and ESPD (e.g., criteria extension) with eIDAS 2.0 wallets.	Medium risk Process is well documented and described the past years. However, current legal provisions on evidences will be a challenge
2.2	**Maturity of needed infrastructure**	Pilot is building upon existing production systems and leveraging previous work conducted at national level. The authentic source is included.	Low risk in the Norwegian, and perhaps Nordic, context.
2.3	**Links to standardization and**	The pilot builds upon the latest ESPD v3.3 data model. However, there is notable absence of	High risk EWC is developing the

	governance initiatives	attestation standardization, with existing legal frameworks being predominately PDF based. There is a need for a European standardization norm for attestations, specifically in areas such as tax certificates. EWC is ahead and could contribute to that.	standards, but their timely adoption is not certain. New domain standards for evidences will be needed. On the positive side, EWC can set best practices as de facto standards directly into the market
2.4	**Market adoption and take-up potential**	The architecture of digital wallets mirrors traditional paper-based processes. This inherent similarity will simplify the adoption and user familiarity.	Medium risk There could be some adoption in Norway and perhaps elsewhere in the Nordics, but the legal challenges remain particularly for cross-border cases.
3	**IMPLEMENTATION**		
3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs and capabilities and can establish credible pilots	Low risk
3.2	**Commitment of participants in all roles foreseen**	Evidence issuer is identified (tax evidence) but no commitment yet.	Medium risk
3.3	**Progress against stated goals**	Stakeholder identification has been done and a pilot timeline is currently being worked on.	Medium risk Pilot implementation not started yet.

5.2 P1.1.2 Automated verification of Economic Operator identity in the procurement process (ESPD) qualification sheet

CRITERIA		Assessment for suitability and feasibility	Risk analysis
1	**Relevance**		
1.1	**Relevance to EU/domain legislation/policy**	Strong relevance and alignment with the European Union's established legal framework that governs public procurement, notably Directive 2014/24/EU, Directive 2014/25/EU, and Directive 2014/23/EU alongside the ESPD. These directives aim to enhance the procurement processes through simplified procedures, while combating corruption and fraud. Advancements such as eIDAS 2.0 and the utilization of digital wallets facilitate the provision of company data from trusted	Low risk Since the pilot focuses on identification, authentication and authorization of the Economic Operator and does not include the exchange of evidences, there is no overlap or conflict with the OOTS. In fact, there is complementarity because the OOTS is lacking

Co-funded by the European Union

		sources, thereby reinforcing trust and automation in procurement transactions.	exactly these features that the pilot focuses on.
1.2	**Relevance to national policy and MS support**	Strong relevance to the National Public Procurement Strategy in Greece (NPPS) for 2021-2025 which includes the digitalization of public procurement processes and improvements in governance. The pilot will showcase how this can be achieved in an efficient way using the wallet architecture. It will also act as potential input to the ongoing work of renewing the national public procurement legislation.	Low risk The pilot engages the only eProcurement platform in Greece and there will be legal person wallets issued by GRNET.
1.3	**Relevance to market needs**	Strong alignment with market needs, specifically in addressing the simplification of public procurement processes, a need that has been extensively studied and highlighted in recent years. (Single Digital Market)	Medium risk The cooperation of Economic Operators cannot be taken as given, unless there is some kind of mandate.
1.4	**Cross-border scope**	The pilot can examine potential cross-border scenarios and synergies in which a Norwegian company uses a wallet to share evidence to the Greek ESPD service.	Medium risk If no cross-border partners or other countries are fund, it will end up being a national pilot.
2	IMPACT		
2.1	**Maturity of business process and infrastructure**	The business process is mature, well researched and documented. Prior work serves as a robust foundation for further development and expansion (PEPPOL, e-SENS, TOOP). The evolution of eProcurement can be influenced through the interconnection of eForms, eCertis and ESPD (e.g., criteria extension) with eIDAS 2.0 wallets.	Low risk Process is well documented and described the past years.
2.2	**Maturity of needed infrastructure**	Pilot is building upon existing production systems and leveraging previous work conducted at national level	Medium risk State authorities are involved as tendering system, but wallet infrastructure is non-existent in the market.
2.3	**Links to standardization and governance initiatives**	Notable absence of standardization, with existing frameworks being predominately PDF based. Need for a European standardization effort for attestations. Organisation wallet and attestation standards do not exist and EWC needs to define them, but EWC proposals may not be included in the ARF in due time (or not at all). This point is relevant to all EWC pilots.	High risk EWC is developing the standards, but their timely adoption is not certain. On the positive side, EWC can set best practices as de facto standards directly into the market.

2.4	**Market adoption and take-up potential**	To increase take-up potential, it is crucial to ensure that wallets are readily available and companies and other registries need to sign up and become familiar with the new technologies.	Medium risk Wallets are not widely available yet and companies are reluctant to be the first who test new technologies and share their real data.
3	**IMPLEMENTATION**		
3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs and capabilities and can establish credible pilots	Low risk The main relying party is already a beneficiary and committed.
3.2	**Commitment of participants in all roles foreseen**	GRNET will provide the wallet and the tendering system is already in the project.	Low risk
3.3	**Progress against stated goals**	Stakeholder identification has been done and a pilot timeline is currently being worked on. No prior work with wallets in the area with the stakeholders, so there is a dependency on other parts of EWC for technology supply.	Medium risk Implementation not started as work at technology level elsewhere in EWC needs to be completed first.

5.3 P2.1.1 Onboarding new Business Partner qualification sheet

	CRITERIA	Assessment for suitability and feasibility	Risk analysis
1	**Relevance**		
1.1	**Relevance to EU/domain legislation/policy**	The business scenario is quite general and may include different cases where a new business partner (supplier/customer) is being onboarded. Although the master data management is not governed by specific laws or EU directives, the KYS pilot aids in the implementation of the Company Law Directive's initiatives regarding the use of digital tools and the digitization of company processes. The 2023 announcement of a revision to Directive 2019/1151/EU augments and broadens its scope in light of recent developments in technology, economy, and society. The piloting of ODI wallets in KYS procedures can enhance compliance to company law related obligations through the promotion of trust and efficiency, as well as the development of a competitive and diverse digital identity ecosystem foreseen in eIDAS 2.0.	Low risk There are not any conflicts with current or upcoming EU legislation.
1.2	**Relevance to national policy and MS support**	National priorities and focus lie on PID and its implications for natural person scenarios. However, while ODI/LPID itself may not be designated as national priority in many Member	Low risk from a relevance perspective due to interconnection with PID related national initiatives

Co-funded by the European Union

		states just yet, it intersects with PID-related national initiatives. This interconnectedness underscores the importance of leveraging resources across various initiatives. Additionally, the relevance of KYS procedures is reinforced by several laws in France, including Loi Sapin 2 which mandates companies to implement corruption prevention measures that may include supplier verification. Furthermore, compliance with AML and terrorism financing regulations, such as LCB-FT, necessitates supplier identity verification. Moreover, the "Loi sur le devoir de vigilance des societes" obliges companies to establish vigilance plans to prevent human rights and environmental abuses, extending the scope of KYS procedures to encompass ethical considerations in supplier relationships.	and French laws that imply the need for automated KYS procedures establishment.
1.3	**Relevance to market needs**	Any effort to digitize and automate KYS will bring immediate benefits to the B2B market in every country. In this scenario, the pilot will implement IBAN attestation and LPID identification and authorization, with a primary focus on establishing trust and enhancing security measures. French banks have shown interest in the KYS pilot, while companies prioritize elements such as trust, information verification, and secure information exchange as critical factors for risk mitigation and fraud prevention. Concerns such as the presence of fake IBAN numbers or counterfeit legal representatives underscore the necessity for automated verification processes. Additionally, there is a shared goal of reducing both costs and time associated with ensuring the accuracy and reliability of business partner information. Thus, the KYS pilot emerges as pivotal for closing the gap when it comes to trust, security, and efficiency establishment within supplier relationships.	Medium risk The pilot has already piqued the interest of banks and companies. In fact, it is one of the most successful EWC pilots so far, from the recruitment perspective. However convincing a large number of actors to engage and allocate/commit resources remains challenging.
1.4	**Cross-border scope**	The pilot has successfully recruited French companies with significant earnings, many of whom engage in business transactions with cross-border suppliers. An essential objective of the pilot is to ensure interoperability with other wallets, facilitating seamless interactions across diverse platforms. Furthermore, efforts to establish favorable relations with foreign Business Registries are underway (namely Sweden, the Netherlands and Germany), enhancing the collaboration for potential cross-border scenarios and synergies.	Medium risk Wallet interoperability is a pre-condition for cross-border interoperation. We are not there yet, but this is the explicit goal.
2	**IMPACT**		

2.1	**2.1 Maturity of business process and infrastructure**	The KYS process is quite routinely executed by companies in every country, so it is fairly mature. That said, EWC will focus mostly on certain initial elements, to show what is possible. While there is no prior work in EU level in this domain, a thorough comprehension of market operations and a clear awareness of the necessary requirements is present. The French market exhibits a level of maturity in its operations, complemented by the EU legislation on procurement. Through proactive engagement with recruited companies, the pilot gathers invaluable insights into their specific needs and requirements for implementing KYS procedures. This collaborative approach ensures that all relevant information and documentation are meticulously collected, allowing for the development and alignment of the pilot with the demands of the market and legislation landscape.	Medium risk There is no prior work at a national or EU level. Requirements and documentation are collected directly from the businesses and actors that do KYS procedures and are aware of what is required. There is scarcity of attestation providers, but the types of attestations that are required are well understood.
2.2	**Maturity of needed infrastructure**	Authentic sources like banks are capable of providing IBAN attestations, and the French business register will provide LPID so a minimum of infrastructure exists. However, for a wider implementation of KYS requirements there is a need for attestations issued by state authorities, a facet currently not addressed within the pilot. To bridge this gap, efforts are underway to develop auto-signage capabilities of attestations. Additionally, Archipels operates their own infrastructure leveraging prior work conducted to address other market needs (document certification). Archipels continues to build upon its existing infrastructure and work on its interoperability with Trace4EU and EWC.	Medium risk State authorities are involved as authentic source, but wallet infrastructure is non-existent in the market.
2.3	**Links to standardization and governance initiatives**	There is no existing standardization and the related EWC work is in progress but at the time of writing not fully documented and available to the pilots. Schemas and rule books need to be provided for the attestations. Opportunity for EWC to fill this gap. Organisation wallet and attestation standards do not exist and EWC needs to define them, but EWC proposals may not be included in the ARF in due time (or not at all). This point is relevant to all EWC pilots.	High risk EWC is developing the standards, but their timely adoption is not certain. On the positive side, EWC can set best practices as de facto standards directly into the market.
2.4	**Market adoption and take-up potential**	Good signals from companies that are going to be part of the pilot. However, asking companies to test first new infrastructure and technologies is always challenging Moreover, change in legislation regarding the acceptance of such procedures is also necessary.	Medium risk Companies are reluctant to be the first to test new technologies.
3	**IMPLEMENTATION**		

Co-funded by
the European Union

3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs and capabilities and can establish credible pilots.	Low risk from an implementation feasibility perspective.
3.2	**Commitment of participants in all roles foreseen**	Commitment from Archipels and recruited companies. Banks has also expressed interest and could be involved in the pilot as the authentic source of the IBAN attestation.	Low risk from an implementation feasibility perspective.
3.3	**Progress against stated goals**	Stakeholder identification and recruitment has already started. A plan is established to also enlist suppliers.	Low risk from an implementation feasibility perspective.

5.4 P2.2.1 Open a bank account for a business qualification sheet

CRITERIA		**Assessment for suitability and feasibility**	**Risk analysis**
1	**Relevance**		
1.1	**Relevance to EU/domain legislation/policy**	Strong relevancy to AML regulations aimed at preventing illegal activities such as money laundering or fraud. By automating and digitizing the KYC processes during the opening of bank accounts, the pilot can significantly benefit banking institutions to meet the strict requirements set forth by AML.	Low risk Building on Nordic Smart Government and Business pilot, there is public sector involvement.
1.2	**Relevance to national policy and MS support**	The EWC pilot aligns with existing national policies and initiatives. Notably, there is already a national pilot in place, and the EWC serves to extend the established national framework to encompass cross-border transactions.	Low risk Building on Nordic Smart Government and Business pilot, there is public sector involvement.
1.3	**Relevance to market needs**	Interviews with banks have revealed that KYC processes are not only costly but also cumbersome and time consuming, especially in cross-border settings. This acknowledgment underlines the urgent need for automation of the process in a way that is secure and reliable.	Medium risk Convincing a large number of actors to engage and allocate/commit resources remains challenging.
1.4	**Cross-border scope**	The pilot will expand an existing national KYC project to encompass cross-border transactions. The Netherlands and Germany involved in the pilot.	Medium risk Cross-border exchanges will be more of a challenge for the pilot.
2	**IMPACT**		
2.1	**Maturity of business process and infrastructure**	The process is well documented and described.	Low risk Building on Nordic Smart Government and Business pilot,

Co-funded by the European Union

			there is public sector involvement.
2.2	**Maturity of needed infrastructure**	Pilot is building upon and leveraging previous endeavors conducted at a national level. Walt-id has been deployed and utilized. Within a controlled test environment, a server-based wallet has been established, facilitating the presentation of attestations by participating companies. Additionally, an issuer exists, enabling the issuance of registration certificates and annual accounts for companies registered.	Low risk Building on Nordic Smart Government and Business pilot, there is public sector involvement.
2.3	**Links to standardization and governance initiatives**	There is no existing standardization and the related EWC work is in progress but at the time of writing not fully documented and available to the pilots. Schemas and rule books need to be provided for the attestations. Opportunity for EWC to fill this gap. Organisation wallet and attestation standards do not exist and EWC needs to define them, but EWC proposals may not be included in the ARF in due time (or not at all). This point is relevant to all EWC pilots.	High risk EWC is developing the standards, but their timely adoption is not certain. On the positive side, EWC can set best practices as de facto standards directly into the market.
2.4	**Market adoption and take-up potential**	Reluctancy for companies to be the first testing new infrastructure and technologies. Banks have expressed interest.	Medium risk As of now, everything runs in a test environment with fictional companies. Hesitation to provide real product data of Finish Business Registry to the wallet provider.
3	**IMPLEMENTATION**		
3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs and capabilities and can establish credible pilots.	Low risk
3.2	**Commitment of participants in all roles foreseen**	Commitment from the Finnish, German and Dutch side. Banks are not enabled yet but have shown interest. Everything runs in a lab environment	Medium risk
3.3	**Progress against stated goals**	An investigation on whether real product data can be used during the pilot is necessary. Banks are not yet involved in EWC but may have to integrate them.	Medium risk Implementation has not started.

Co-funded by
the European Union

5.5 P3.1.1 Domain holder verification by domain registry qualification sheet

CRITERIA		Assessment for suitability and feasibility	Risk analysis
1	Relevance		
1.1	**Relevance to EU/domain legislation/policy**	Strong relevancy to European Directive NIS2 (December 2022) in which Article 28 introduced new obligations for domain registries and registrars about establishing identity verification procedures of domain holders. Notably, the directive advocates for electronic identity solutions as a viable means to address these requirements effectively. Piloting the EUDIW, the adoption of electronic identity verification gets facilitated thereby contributing to the efforts on fulfilling obligations put on entities in the domain registration ecosystem across Europe.	Low risk No conflicts, high market value.
1.2	**Relevance to national policy and MS support**	Not applicable. Users originate from all over Europe and not limited to 1 MS support.	Low risk No conflicts or contradicting national legislations.
1.3	**Relevance to market needs**	Domain Registries can benefit by the use of EUDIW as authentication means for the registrie's domain holder portals. Moreover, due to NIS2 the domain registries are required to confirm that registration data about domain holder are accurate. The Domain Registrars currently don't provide any information about authenticity of data provided by domain holders and piloting the EUDIW Domain can fill this gap.	Medium risk Pilot doesn't have any QSTP involved yet.
1.4	**Cross-border scope**	The pilot's scope is cross-border, since every domain registry allows cross-border registrations. The pilot will demonstrate how users from other countries should use their wallets to communicate to CZ.NIC registry.	Medum risk Cross-border participation must be ensured
2	IMPACT		
2.1	**Maturity of business process and infrastructure**	The process is well described and documented, with a strong foundation based on the requirements outlined in the European Directive NIS2. Building upon prior work done as part of a broader initiative involving four registries from the Netherlands, Denmark, Estonia and Czech Republic, where progress has been made in leveraging eIDAS 1.0 eIDs to	Low risk

Co-funded by the European Union

		establish connections with these registries. However, while certain aspects of the registries were succesfully integrated into the eID network, challenges remained in resolving the organizational identity. EWC and ODI piloting aims to effectively address this gap.	
2.2	**Maturity of needed infrastructure**	The limitations of eIDAS 1.0 architecture hindered the seamless integration of registries. With the introduction of eIDAS 2.0 reference implementation, CZ.NIC trust services are relaunching to utilize wallets technology aiming to be used more widely in relation with eIDAS 1.0 and building upon work done prior to EWC (RegeID).	Low risk
2.3	**Links to standardization and governance initiatives**	There is no existing standardization and the related EWC work is in progress but at the time of writing not fully documented and available to the pilots. Schemas and rule books need to be provided for the attestations. Opportunity for EWC to fill this gap. Organisation wallet and attestation standards does not exist and EWC needs to define them, but EWC proposals may not be included in the ARF in due time (or not at all). This point is relevant to all EWC pilots	High risk EWC is developing the standards, but their timely adoption is not certain. On the positive side, EWC can set best practices as de facto standards directly into the market
2.4	**Market adoption and take-up potential**	To increase take-up potential, it's crucial to ensure that wallets are readily available and companies and other registries need to sign up and become familiar with the new technologies.	Medium risk Wallets are not widely available yet and companies are reluctant to be the first who test new technologies.
3	**IMPLEMENTATION**		
3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs, and capabilities. The extended business scenario description is missing.	Medium risk CZ.NIC will not use the reference implementation wallet but create their own.
3.2	**Commitment of participants in all roles foreseen**	CZ.NIC is committed and identified possible stakeholders	Medium risk A strategy for recruiting companies must be defined
3.3	**Progress against stated goals**	Deployed a relying party portal interface that uses QR code to ask for PID/LPID.	High risk CZ.NIC aims to create their own wallet implementation

Co-funded by
the European Union

5.6 P3.2.1 Domain ownership as credential for QWAC issuance qualification sheet

CRITERIA		Assessment for suitability and feasibility	Risk analysis
1	Relevance		
1.1	**Relevance to EU/domain legislation/policy**	Strong relevancy to European Directive NIS2 (December 2022) in which Article 28 introduced new obligations for domain registries and registrars about establishing identity verification procedures of domain holders. Notably, the directive advocates for electronic identity solutions as a viable means to address these requirements effectively. Piloting the EUDIW, the adoption of electronic identity verification gets facilitated thereby contributing to the efforts on fulfilling obligations put on entities in the domain registration ecosystem across Europe.	Low risk No conflicts, high market value.
1.2	**Relevance to national policy and MS support**	Not applicable. Users originate from all over Europe and not limited to one MS support.	Low risk No conflicts or contradicting national legislations
1.3	**Relevance to market needs**	Domain registries and QSTPs issuing QWAC certificates use cumbersome identity and domain ownership checks and tools like WHOIS services and publishing DNS records. These tools can be replaced by having Domain Ownership as credential in the wallet. The QSTP issuing QWAC can streamline the identity verification of the requester and domain ownership necessary prior to the certificate issuance by taking advantage the PID + Domain Ownership credentials stored in wallets	Medium risk Pilot doesn't have any QSTP involved yet.
1.4	**Cross-border scope**	A cross border scenario is examined where Italian authorities can issue a certificate in a registry of Czech for a German person.	Medium risk Wallet interoperability is a pre-condition for cross-border interoperation. We are not there yet, but this is the explicit goal.
2	IMPACT		
2.1	**Maturity of business process and infrastructure**	The QWAC issuance is a well described and documented process.	Low risk
2.2	**Maturity of needed infrastructure**	The existing infrastructure is already equipped with the means to issue credentials directly into the wallet. There is an issuance and	Low risk

Co-funded by the European Union

		verification interface already in place that can be integrated with the EUDIW.	
2.3	**Links to standardization and governance initiatives**	There is no existing standardization and the related EWC work is in progress but at the time of writing not fully documented and available to the pilots. Schemas and rule books need to be provided for the attestations. Opportunity for EWC to fill this gap. Organisation wallet and attestation standards does not exist and EWC needs to define them, but EWC proposals may not be included in the ARF in due time (or not at all). This point is relevant to all EWC pilots	High risk EWC is developing the standards, but their timely adoption is not certain. On the positive side, EWC can set best practices as de facto standards directly into the market
2.4	**Market adoption and take-up potential**	Good signals from companies that are going to be part of the pilot. However, asking companies to test first new infrastructure and technologies is always challenging.	Medium risk Companies are reluctant to be the first who test new technologies. Moreover, change in legislation regarding the acceptance of such procedures is also necessary.
3	**IMPLEMENTATION**		
3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs, and capabilities. The extended business scenario description is missing.	Medium risk from an implementation feasibility perspective is not assured.
3.2	**Commitment of participants in all roles foreseen**	Discussions with Infocert to act as QSTP but no commitment yet. A Domain Registrar is also missing.	High risk Pilot participants do not seem to be fully committed yet.
3.3	**Progress against stated goals**	Stakeholder identification and recruitment has already started.	High risk Feasibility to be confirmed.

5.7 P4.1.1 Peppol network registration and use qualification sheet

CRITERIA		Assessment for suitability and feasibility	Risk analysis
1	**Relevance**		

Co-funded by
the European Union

1.1	**Relevance to EU/domain legislation/policy**	The pilot is relevant to the new Company Law Directive, particularly in its alignment with eIDAS 2.0 standards and its emphasis on digitizing processes and company registration attestations. As outlined in the directive, the EUDIW serves as a vital component in supporting the digitization efforts by providing a secure and reliable platform for managing digital identities and attestations.	Low risk The pilot is aligned with the Peppol Internal Regulation, the Policy for Entity Identification.
1.2	**Relevance to national policy and MS support**	Not applicable. Users originate from all over Europe and are not limited to one MS support. This means that there are no showstoppers either, and the pilot is relevant in all countries (all EU countries are already in Peppol)	Low risk The pilot is aligned with the Peppol Internal Regulation, the Policy for Entity Identification.
1.3	**Relevance to market needs**	Strong alignment with market needs, specifically in addressing the simplification of KYC processes, a need that has been highlighted in the new Company Law Directive	Medium risk The introduction of wallets is new in this market, where Service provider offerings are tightly measured and cost structures challenging.
1.4	**Cross-border scope**	Peppol is present in all EU countries and in 41 countries globally. INVINET has end-users in all European Countries but will focus more on France, Sweden and the Netherlands.	Medium risk It will be difficult for a Service Provider to work with the same wallet provider in more than one country, but this should be attempted.
2	IMPACT		
2.1	**Maturity of business process and infrastructure**	The business process is mature and well documented. The Peppol Internal Regulations provide a basis for hundreds of Peppol Service Providers conducting KYC on a regular basis.	Low risk Process is well documented and described the past years.
2.2	**Maturity of needed infrastructure**	Pilot is building upon existing systems in production. Relationships with wallet providers (as in France) are already built.	Medium risk State authorities are not involved within the pilot and links to authentic sources depend on what the wallet providers do
2.3	**Links to standardization and governance initiatives**	There is no existing standardization and the related EWC work is in progress but at the time of writing not fully documented and available to the pilots. Schemas and rule books need to be provided for the attestations. Opportunity for EWC to fill this gap. Organisation wallet and attestation standards do not exist and EWC needs to define them,	High risk EWC is developing the standards but their timely adoption is not certain. On the positive side, EWC can set best practices as de facto standards directly into the market.

		but EWC proposals may not be included in the ARF in due time (or not at all). This point is relevant to all EWC pilots.	
2.4	**Market adoption and take-up potential**	To increase take-up potential, it is crucial to ensure that wallets are readily available and companies and other registries need to sign up and become familiar with the new technologies.	Medium risk Wallets are not widely available yet and companies are reluctant to be the first to test new technologies and share their real data.
3	**IMPLEMENTATION**		
3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs and capabilities and can establish credible pilots.	Low risk
3.2	**Commitment of participants in all roles foreseen**	Commitment from OpenPeppol and INVINET.	Medium risk Probable links to more wallet providers may be needed.
3.3	**Progress against stated goals**	Stakeholder identification has been done and a pilot timeline is currently being worked on.	Low risk Pilot implementation in France already started.

5.8 P4.2.1 Verifiable eReceipt qualification sheet

CRITERIA		Assessment for suitability and feasibility	Risk analysis
1	**Relevance**		
1.1	**Relevance to EU/domain legislation/policy**	No specific legislation is governing vReceipts. However, this lack of regulatory framework means there are no conflicts with existing EU legislation. The pilot is breaking new ground in B2C standardization.	Medium risk There is risk in pioneering a standard, but it is manageable because it reuses the EN and the Peppol CIUS.
1.2	**Relevance to national policy and MS support**	The Finnish Real Time Economy program has run a technical pilot and produced multiple deliverables to specify what verifiable eReceipts are and how should they be used with wallets and other systems. The EWC pilot serves as a natural extension of the groundwork laid during the RTE program, enhancing, and complementing its objectives.	Low risk Good support by the Tax Authority, no conflicts with other obligations.
1.3	**Relevance to market needs**	Present implementations of digital receipts operate on proprietary platforms, lacking interoperability among service providers. This fragmentation in the market restricts scalability and no integrity/authenticity safeguards are in	Low risk

Co-funded by the European Union

		place. Verifiable eReceipts address these shortcomings and B2C-B2B stakeholders can significantly benefit from the use of EUDIW.	
1.4	**Cross-border scope**	Cross-border exchanges will be a challenge but there is already a very good connection to the travel use case and pilot synergies with Greek Ferries company for cross-border piloting.	Low risk Cross-border plans already in place.
2	IMPACT		
2.1	**Maturity of business process and infrastructure**	The eReceipts are well described and defined in previous endeavors during the RTE program.	Medium risk Standardized B2C receipts is a new process, there is no extensive international experience.
2.2	**Maturity of needed infrastructure**	Pilot is building upon and leveraging previous endeavours conducted at a national level.	Medium risk Standardized B2C receipts is a new process, there is no extensive international experience.
2.3	**Links to standardization and governance initiatives**	There is no existing standardization and the related EWC work is in progress but at the time of writing not fully documented and available to the pilots. Schemas and rule books need to be provided for the attestations. Opportunity for EWC to fill this gap. Organisation wallet and attestation standards does not exist and EWC needs to define them, but EWC proposals may not be included in the ARF in due time (or not at all). This point is relevant to all EWC pilots.	High risk EWC is developing the standards, but their timely adoption is not certain. On the positive side, EWC can set best practices as de facto standards directly into the market.
2.4	**Market adoption and take-up potential**	Reluctancy for companies to be the first testing new infrastructure and technologies.	Medium risk As of now, everything runs in a test environment with fictional companies. Hesitation to provide real product data of Finnish Business Registry to the wallet provider.
3	IMPLEMENTATION		
3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs and capabilities and can establish credible pilots.	Low risk

Co-funded by the European Union

3.2	**Commitment of participants in all roles foreseen**	Commitment from the Finnish side and discussions with Greek company (Ferries) to undertake the role of the Merchant.	Medium risk
3.3	**Progress against stated goals**	Implementation has started in national level.	Low risk Implementation has started.

5.9 P4.3.1 Create a company branch in another country qualification sheet

CRITERIA		Assessment for suitability and feasibility	Risk analysis
1	**Relevance**		
1.1	**Relevance to EU/domain legislation/policy**	The pilot holds significant relevance to the new Company Law Directive, particularly in its alignment with eIDAS 2.0 standards and its emphasis on digitizing processes and company registration attestations. As outlined in the directive, the EUDIW serves as a vital component in supporting the digitization efforts by providing a secure and reliable platform for managing digital identities and attestations. Furthermore, the pilot addresses potential overlaps with the OOTS and BRIS when retrieving evidence for company registration. While OOTS and BRIS focus on gathering evidence through an eDelivery system, the EUDIW takes a user-centric SSI approach. This fundamental difference allows the EUDIW to bridge the gap in authentication and verification, offering an alternative method that complements existing approaches by empowering users with greater control over their identities. By piloting the EUDIW alongside OOTS and BRIS, the pilot not only fills existing gaps but also introduces a novel approach to identity management and verification.	Medium risk Overlap with OOTS and with BRIS, previous attempts to digitize this use case at an EU level. This is particularly true when it comes to the exchange of evidences. That said, the LPID part, however, is complementary to OOTS.
1.2	**Relevance to national policy and MS support**	The pilot supports the implementing act of eIDAS 2.0. While there is overlap with existing Swedish eIdentification, the pilot's objectives are not contradictory but rather complementary.	Medium risk Overlaps with Swedish electronic identity. Legislation adjustments may be needed e.g. recognize digital attestations as equivalent to traditional paper-based documents certified by notaries.

Co-funded by the European Union

1.3	**Relevance to market needs**	The urgency of expediting the business establishment is undeniable. Traditionally, company registration processes, especially cross-border, have been hindered by bureaucracy and cumbersome procedures. Automating company registration processes addresses critical market needs and streamlines operations.	Low risk In Sweden, the stakeholders are aligned and there can be acceptance.
1.4	**Cross-border scope**	The pilot inherently involves cross-border processes by default, focusing on collaboration between the Swedish Business Registry and its Norwegian counterpart. As the pilot progresses, there is an opportunity to include more Business Registries.	Medium risk Take up is possible in the Swedish, and maybe Nordic, context. However, the use case is by definition cross-border, so companies from other countries need to be found.
2	IMPACT		
2.1	**Maturity of business process and infrastructure**	The business process is quite well analyzed and well described. Ongoing requirement analysis by lawyers to make it compatible both with eIDAS 2.0 and the new Company Law Directive.	Low risk
2.2	**Maturity of needed infrastructure**	Yet, relying parties do not have organizational wallets. Considerations regarding the potential of Business Registers to facilitate not only the issuance of attestations but also the provision of wallets themselves; upon formation of a company, a wallet is automatically assigned to it.	Medium risk Processes that require high LoA are not possible yet with existing national legislation
2.3	**Links to standardization and governance initiatives**	There is no existing standardization and the related EWC work is in progress but at the time of writing not fully documented and available to the pilots. Schemas and rule books need to be provided for the attestations. Opportunity for EWC to fill this gap. Organisation wallet and attestation standards does not exist and EWC needs to define them, but EWC proposals may not be included in the ARF in due time (or not at all). This point is relevant to all EWC pilots	High risk EWC is developing the standards, but their timely adoption is not certain. On the positive side, EWC can set best practices as de facto standards directly into the market
2.4	**Market adoption and take-up potential**	Awareness is not very high right now.	Medium risk Companies are not widely aware and there is a gap going into production with new technologies
3	IMPLEMENTATION		

Co-funded by
the European Union

3.1	**Completeness of scenario/pilot plan description**	The piloting partner and participating organizations are aware of the domain, their specific needs and capabilities and can establish a credible pilot. Comprehensive documentation about the pilot exists and there is also a plan about recruiting Norwegian companies	Low risk
3.2	**Commitment of participants in all roles foreseen**	The business registries are attestation issues themselves. Plan to recruit Norwegian companies to open businesses in Sweden but may be challenging.	Medium risk There may be no incentives for Norwegian companies to open branches in Sweden.
3.3	**Progress against stated goals**	Scoping things out, not ready yet to involve/invite others.	Low risk Implementation already started

6 Pilot status at month M15

6.1 State of implementation

The following table presents the state of the pilots based on the monitoring states established in section 2.4.

Pilot name	**Status**
P1.1.1: Issue and verify attestations for evidence in the procurement process (ESPD)	Pilot committed; implementation not started
P1.1.2: Automated verification of EO identity in the procurement process (ESPD)	Pilot committed; implementation not started
P2.1.1 Onboarding new business partner	Implementation in progress
P2.2.1 Open a bank account for a business	Pilot committed; implementation not started
P3.1.1 Domain holder verification by domain registry	Pilot committed; implementation not started
P3.2.1 Domain ownership as credential for QWAC issuance	Commitment to fully confirm
P4.1.1 Peppol network registration and use	Implementation in progress
P4.2.1 Verifiable eReceipt	Implementation in progress
P4.3.1 Create a company branch in another country	Implementation in progress

Four out of nine pilots have started active implementation (green colour). The rest are committed and are expected to start soon, and only one (P3.2.1 Domain ownership as credential for QWAC issuance) is assessed as showing a high risk of not materializing.

Co-funded by the European Union

7 Conclusions

The main conclusions from the first year of piloting in EWC as described in deliverable D3.5, can be summarized as follows:

1. Pilot identification and relevance
    a. We identified eight (8) Business Scenarios and nine (9) pilots in total, spanning across all the four (4) Business Areas included in the initial scope and we found the pilots identified to be of good value, following an objective assessment methodology.
    b. In most cases, there is a 1 to 1 correspondence between business scenarios and pilot plans. The reason is that the business scenarios are focused on different aspects of certain business processes such as KYC and KYS, rather than following a function-oriented categorization.
    c. The pilot designers and promoters preferred to give emphasis to the business goals of each scenario rather than group them on technical capabilities or abstract business functions. As pilots proceed into implementation and it becomes clearer what is actually being piloted in each case, we will provide such groupings, particularly related to capabilities.
    d. Pilot identification by the project beneficiaries is in some cases a bit narrow, which explains the fragmentation into smaller segments of what may be considered more extensive business processes in the market. The reason for this approach is that ODI is still a new concept and EWC in many ways is breaking new ground by introducing new generation EUDI compliant Legal Person wallets with LPID into business processes that are now manual or otherwise digitized in a non-standardized manner. So, it is understandable that the approach in these initial pilots is more conservative.
    e. What is now included in D3.5 is a first group of pilots already identified and on their way to implementation. There are additional pilot prospects in some of the business scenarios, such as in Business Document Exchange, where more detailed pilot plans may be submitted in the second part of the project. If so, these will be included in future versions of this deliverable.
2. Pilot impact, risks, and adoption potential
    a. Most of the pilots have a good relevance to business needs and as such they can have market potential. That said, the initial engagement of the user community is still rather limited, because this is new functionality and infrastructure, and legal person wallets are not yet in the market.
    b. Most pilots have a rather local focus, at least initially. But all aspire to a wider and more cross-border expansion of operations and will cooperate amongst themselves in order to cross-benefit from participant recruitment to the best of their abilities. So, the scope is expected to increase, but of course this remains to be verified in the second part of the project.
    c. Most risks in the pilots have to do with new functionality and infrastructure that may hinder widespread adoption. This is something that all Large-Scale Pilots face but in EWC in particular, the small size of the project overall and the fact that ODI plots have a limited part of a small project does affect the ability of partners to engage a wider range of participants.
    d. The highest risk lies with standardization. EWC is ahead of the curve when it comes to ARF so creates the standards and has to pilot before these are adopted. This is a challenge both because implementers are waiting for basic building blocks such as EWC compliant wallets to be available, and because what is implemented may not end up being adopted by standardization efforts. This is of course a risk that most

Co-funded by
the European Union

Large-Scale Pilots face when they have a mismatch between their project timing and that of standardization or legislation.

   e. In some pilots, such as in Public Procurement or opening a branch abroad, EWC is actually overhauling current practices and even prior European initiatives, by using ODI and legal person wallets to attempt a more efficient digitization of certain business processes. This is a conscious risk, but it is worth doing at least some exploratory work that would need legal environment and market infrastructure to evolve from their current state.

3. Pilot implementation and monitoring
   a. A comprehensive methodology for pilot definition, assessment and monitoring has been adopted, based on experience from previous LSPs. This methodology has been used for the analysis in deliverable D3.5, and will be the basis for monitoring the evolution of pilot implementation and conclusion along the stages of the pilot lifecycle.
   b. At the time of writing (June 2024), 4 out of 9 pilots have started active implementation, the rest are committed and are expected to start soon, and only one is assessed as showing a high risk of not materializing.
   c. Further editions of this deliverable will be produced internally at the end of September and end of December 2024, reflecting the progress of pilots at those points in time.