



WE BUILD
CONSORTIUM

Deliverable D2.1

Pilot Design

Version: 1.0
July 2026



Co-funded by
the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Project and document data

Item	Description
Project title	W allet E cosystem for B usiness and BUSINESS and PAYMENTS U se cases on I dentification, L egal representation and D ata sharing
Grant Agreement no	Project 101224751 — WE BUILD
Deliverable title	D2.1 Pilot Design
Deliverable type	R – Document, report
Responsible party	Stichting ICTU
Authors	Andriana Prentza, Xavier Juredieu, Ard van der Heijden
Contributing parties	InfoGreff GIE, University of Piraeus Research Centre, Stichting ICTU
Reviewers	Marie-José Hoefmans, Frans de Kok, Arno Fiedler, Maria Cristina Timon Lopez, Arthur van der Wees, Dimitra Stefanatou, Franziska Granc, Paloma Llaneza, Joost Fleuren, Stef Haartman, Bob Kronenburg, Rob Brand, Sarah Amandusson, Giulio Messori
Dissemination level	Public

History of changes

Version	Date	Change
0.1	3 June 2026	Setup template and ToC
0.2	30 June 2026	Initial content
0.8	3 July 2026	Internal review completed
0,89	21 July 2026	Internal processing of review completed
0.9	23 July 2026	Processing of review completed – ready for approval
1.0	30 July 2026	Approved for submission

Table of contents

Table of contents	3
1. Executive summary	7
2. Introduction	8
2.1 Scope and goal	8
2.2 Target audience.....	8
2.3 Versioning.....	8
3. Approach of the specification phase	9
3.1 Introduction.....	9
3.2 Phased approach.....	9
3.3 Prioritization	10
3.4 Deliverables and templates	10
3.5 Dependencies	11
3.6 Roles and responsibilities.....	12
3.7 Evaluation strategy.....	12
3.8 Collaboration with other work packages	12
4. Overview of use cases	13
4.1 Business domain	13
4.1.1 Use case BU1 - Know your business partner (supplier/customer/employee)	13
4.1.2 Use case BU2 – Piloting Company Law Directive for Company Branch Creation	16
4.1.3 Use case BU3 – Foreign tax declaration	18
4.1.4 Use case BU4 – A company representative acting and signing on behalf of company.....	21
4.1.5 Use case BU5 – Issue micro Credentials	24
4.1.6 Use case BU6 – Business access to the Once Only Technical System (OOTS)	25
4.2 Supply Chain domain	27
4.2.1 Use case SC1 – Authentication and access for transport	27
4.2.2 Use case SC2 – Trusted data sharing for dataspaces	30
4.2.3 Use case SC5 - eInvoicing	32
5. Scoping decisions and working assumptions	36
5.1 Scoping decisions.....	36
5.2 Main working assumptions	37
6. Expected learnings	39
6.1 Integration of wallet trust into existing operational sector ecosystems.....	39
6.2 Use of attestations as reusable trust anchors across processes	39
6.3 User Management and Delegation of Rights.....	39
6.4 Wallet Dance	39
6.5 Trust infrastructure needs.....	40
6.6 User Experience.....	40
6.7 Attestation Standardization.....	40

6.8	<i>Machine-to-machine</i>	41
6.9	<i>Identifier and discovery reuse</i>	41
7.	Challenges and risks	42
7.1	<i>Introduction</i>	42
7.2	<i>Main challenges</i>	42
7.3	<i>Main risks</i>	43
8.	Conclusion	46
Annex A – Use case / attestation matrix MVP/MVP+		47
Annex B – Use case / country matrix		48
Annex C – MVP scenario specification documents		50

List of figures

Figure 1: Phased approach of the work-package.....	9
--	---

List of tables

Table 1: BU1 - Scenario 1	14
Table 2: BU1 - Scenario 2.....	15
Table 3: BU1 - Scenario 3.....	15
Table 4: BU1 - Scenario 4.....	15
Table 5: BU1 - Scenario 5.....	16
Table 6: BU2 - Scenario 1.....	17
Table 7: BU2 - Scenario 2.....	18
Table 8: BU3 - Scenario 1.....	20
Table 9: BU3 - Scenario 2.....	20
Table 10: BU3 - Scenario 3.....	20
Table 11: BU3 - Scenario 4.....	21
Table 12: BU4 - Scenario 1a	22
Table 13: BU4 - Scenario 1b.....	23
Table 14: BU4 - Scenario 1c	23
Table 15: BU5 - Scenario 1	25
Table 16: BU6 - Scenario 1	26
Table 17: BU6 - Scenario 2.....	27
Table 18: SC1 -Scenario 1.1.....	29
Table 19: SC1 – Scenario 1.2.....	30
Table 20: SC1 - Scenario 1.3	30
Table 21: SC2 - Scenario 1	32
Table 22: SC5 - Scenario 1	34
Table 23: SC5 - Scenario 2.....	35
Table 24: SC5 - Scenario 4.....	35

Abbreviation	Meaning
A1	Portable Document A1 (social security form)
AP	Access Point (Peppol network service provider)
ADR	Architecture Decision Records
ARF	Architecture and Reference Framework
BU	Business (use case prefix)
BU1	Business use case 1 – Know Your Business Partner
BU2	Business use case 2 – Create company branch
BU3	Business use case 3 – Foreign tax declaration
BU4	Business use case 4 – Company representative acting on behalf of company
BU5	Business use case 5 – Micro Credentials
BU6	Business use case 6 – Access to the Once Only Technical System (OOTS)
CEADS	Common European Agricultural Data Space
D2.1	Deliverable 2.1 (Pilot Design)
DC4EU	Digital Credentials for Europe
DCQL	Digital Credentials Query Language
DUNS	Data Universal Numbering System identifier
DSI	Data Space Initiative
DSSC	Data Space Support Centre
EAA	Electronic Attestation of Attributes
EBW	European Business Wallet
EBWOID	European Business Wallet Organisational Identifier
eCMR	Electronic Consignment Note (CMR)
EORI	Economic Operators Registration and Identification number
ESG	Environmental, Social and Governance (indicators)
EUCC	EU Company Certificate
EUDI Wallet	European Digital Identity Wallet
EUDIW	European Digital Identity Wallet
eCMR	Electronic Consignment Note (CMR)
EWC	EU Digital Identity Wallet Consortium
HADEA	European Health and Digital Executive Agency
IBAN	International Bank Account Number
IBAN-OV	IBAN Ownership Verification attestation
ISPS Code	International Ship and Port Facility Security Code
JSON-LD	JavaScript Object Notation for Linked Data
KYC	Know Your Customer
KYB / KYBP	Know Your Business / Know Your Business Partner
KYE	Know Your Employee
KYS	Know Your Supplier
LEI	Legal Entity Identifier
LPID	Legal Person Identification Data
LSP	Large-Scale Pilot
M2M	Machine-to-Machine

MVP	Minimum Viable Product
MVP+	Extended Minimum Viable Product / stretch-goal scope
NOBID	Nordic-Baltic eID
OID4VP	OpenID for Verifiable Presentations
OOTS	Once Only Technical System
PCS	Port Community System
PID	Person Identification Data / credential in the EUDI Wallet
PoA	Power of Attorney
PoE	Power of Employee
PoR	Power of Representation
POTENTIAL	PiLOTs for European digiTal Identity wALlet
PoX	Power of X (generic representation/mandate attestation)
Pub-EAA	Public Electronic Attestation of Attributes
QERDS	Qualified Electronic Registered Delivery Service
QES	Qualified Electronic Signature
QEAA	Qualified Electronic Attestation of Attributes
QR Code	Quick Response code (used for eFTI controls)
QTSP	Qualified Trust Service Provider
RP	Relying Party
RP (matrix)	Relying Party (column in annex matrices)
SC	Supply Chain (use case prefix)
SC1	Supply Chain use case 1 – Authentication and access for transport
SC2	Supply Chain use case 2 – Trusted data sharing for dataspace
SC5	Supply Chain use case 5 – eInvoicing
SD-JWT	Selective Disclosure JSON Web Token
SSO	Single Sign-On
ToC	Table of Contents
TRC	Tax Residency Certificate
TOS	Terminal Operating System
UBO	Ultimate Beneficial Owner
UC	Use Case
VAT	Value Added Tax
VAT ID	Value Added Tax Identification Number
ViDA	VAT in the Digital Age (EU initiative)
WE BUILD	Wallet Ecosystem for Business and BUSINESS and PAYMENTS Use cases on Identification, Legal representation and Data sharing
WP	Work Package
WP2	Work Package 2
WP3	Work Package 3
WP4	Work Package 4
WP5	Work Package 5
WP6	Work Package 6

1. Executive summary

This deliverable presents the pilot design for the business and supply chain use cases that will be executed in Work Package 2 of WE BUILD. It consolidates the results of the initial “stock taking” and subsequent “specification” phases into a coherent set of scenarios and attestation designs that are ready to guide implementation, testing and piloting.

The design results from a two-step process of stock taking and specification. The work identified 44 scenarios in total across WE BUILD, of which 25 high-priority scenarios using 37 high-priority attestation types form the core Minimum Viable Product scope; 17 additional scenarios are retained as stretch goals where capacity and feasibility allow. The specification phase refined these pilot definitions into highly focused and detailed scenario designs, process descriptions, attestation rulebooks and cross-border combinations at a level suitable for implementation teams.

Use cases are grouped into two domains. In the Business domain, pilots address Know Your Business Partner processes, creating a company branch abroad, foreign tax declarations, cross-border representation, micro-credentials and access to the Once Only Technical System. In the Supply Chain domain, pilots focus on authentication and access for transport, trusted data sharing for dataspaces and eInvoicing in trusted buyer–supplier relationships. Together, they cover typical cross-border situations where wallets, attestations and interoperable trust frameworks can support businesses, public authorities, intermediaries and logistics actors.

The pilot design builds on and extends results from previous Large-Scale Pilots (POTENTIAL, NOBID, EWC, DC4EU), reusing existing concepts and components where possible while addressing new challenges such as shared attestations, mandate and representation models, and common wallet and trust infrastructure. Because many use cases depend on the same attestation types and technical components, structured cross-use-case coordination and close collaboration with other work packages, in particular architecture and technology, are essential elements of the approach.

The document also sets out the main learning goals and risks for the pilots. The learning agenda stayed close to the 6 key-objectives of WE BUILD and include attestation multiplicity, user management and delegation, wallet interaction patterns, trust infrastructure needs, user experience and the potential for attestation standardisation across countries and domains. Key risks relate to evolving standards and regulation, multi-country and multi-partner coordination, securing sufficient issuers and relying parties, and delivering meaningful pilots within the available time, especially in complex supply chain environments. These are mitigated through strong prioritisation, active partner engagement, structured change management and continuous monitoring of feasibility and progress.

This deliverable thus serves as the current pilot baseline for Work Package 2. It defines the intended Business and Supply Chain pilot scope and priorities, while allowing for limited adjustments during implementation, testing and piloting, which will be reported in the final work package deliverable rather than through updated versions of this document.

2. Introduction

2.1 Scope and goal

This document is the first formal deliverable of Work Package 2 in WE BUILD and describes the use cases and scenarios that will be piloted in this Work Package. It describes them on a medium/high level, referring to more detailed designs in an external [Annex](#).

The document clarifies what choices were made during designing the use cases in order to find the proper balance between value and feasibility within the 25-month duration of the project. These are strongly related to the key objectives of the project and the learning goals of each use case.

WE BUILD is a very ambitious project. It has a big scope, many partners, many dependencies and many uncertainties. These have been translated to challenges and risks, which are also addressed in this document.

The document aims to be a clear next step in the road from Grant Agreement to actual piloting. It will be used as a guiding star for the next steps in the project: the implementation, testing and piloting. During the implementation all use cases aim for piloting in pre-production, while some may develop towards piloting in closed-production (for which additional measures concerning data-protection will be assessed).

2.2 Target audience

The document is a public deliverable and with that will be of interest for any actor involved in the wallet ecosystem, business in general, transport and related industries after the **European Health and Digital Executive Agency (HADEA)** has accepted the deliverable.

2.3 Versioning

The scope for piloting as described in this document is to be seen as the intention for piloting BUSINESS and SUPPLY CHAIN use cases in WE BUILD. Changes in the scope are expected to a certain (though minimal) extent, being both negative and positive. During implementation, testing and piloting both headwinds and tailwinds are to be expected, bringing the work package to the final set of pilots to execute. Therefore, the Work Package has several additional scenarios available, in case the project can do more than is described in this document.

Any changes in the scope that will be made after submission of this document, will however not result in new versions of this document. The final deliverable of the Work Package will of course reflect any positive and negative changes made, including motivations.

This means that after version 1.0 of this document no additional versions are to be expected.

3. Approach of the specification phase

3.1 Introduction

The pilot design is the result of a two-step approach in which the level of detail of the use cases gradually increased. The result is a design for scenarios to be piloted in the 9 use cases in this work package, that together with the architectural and technical guidance from work package 4 provides sufficient detail for implementation of solutions that support piloting.

3.2 Phased approach

The design was produced in two steps: stock taking and specification. For each phase, the use cases received templates to use for results that had to be produced. Also, the approach for the phase was thoroughly explained, setting out clear boundaries and milestones while also leaving room for use case leads to lead their use cases in ways that fit each individual use case best.

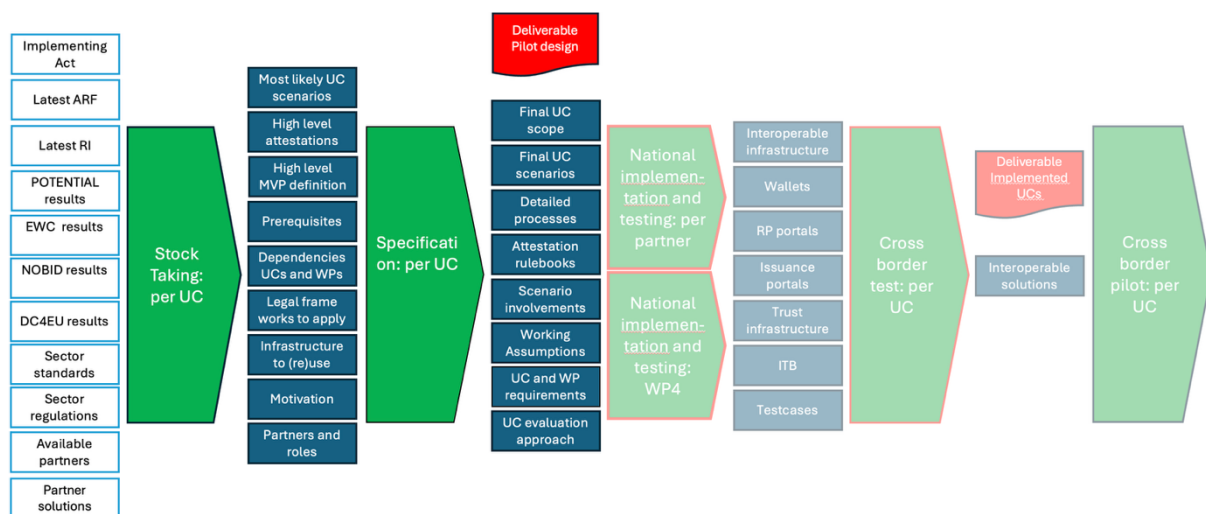


Figure 1: Phased approach of the work-package

An important element of the stock-taking was the assessment of what results of previous LSP could be reused, to efficiently produce the use case. To facilitate this a hand-over day was organized in the beginning of the project where POTENTIAL, EWC, NOBID and DC4EU presented their results to WE BUILD and explained where documentation could be found.

The stock-taking phase transformed the general ideas in the Grant Agreement for each of the nine use cases in Work Package 2 into more concrete 'pilot definitions'. It identified 44 scenarios in total across WE BUILD, of which 25 were classified as high priority using 37 types of high priority attestations. For each identified scenario a description was produced of the initial scope of each scenario, the attestations that were expected to be used, the partners that would be involved, a summary of the legal frameworks and standards.

In the stock-taking phase use cases started to prioritize their scenarios, to find the proper focus throughout the rest of the project.

The specification phase builds directly on the pilot definitions. Its purpose was to turn these into a detailed 'pilot specification' that is concrete enough to guide implementation and piloting. This

means resolving ambiguities, agreeing on step-by-step processes, identifying all required parties and other actors, designing attestations, and documenting cross-border piloting combinations.

3.3 Prioritization

Work in the specification phase was deliberately sequenced. Teams began with their highest prioritized scenarios (called ‘minimum viable product’ scenarios, or MVP) and only move to scenarios with a lower priority (called MVP+) once the work was sufficiently mature. The MVP scenarios are therefore the backbone of the pilot, while MVP+ scenarios are the "stretch-goals." Where capacity is constrained, MVP+ scope can be reduced or deferred without jeopardising the core of the use cases.

Use cases also identified MVP+ elements within some MVP scenarios, to expose the absolute core and sequence implementation more precisely.

The project prioritized working with SD-JWT and mdoc over other potential formats, unless a use case or scenario could clearly motivate why other formats should be used from the beginning. For use cases progressing quickly, working with alternative formats will be considered later in the project. One use case (Supply Chain 2) will work with the JSON-LD format from the start.

Overall the use cases were fully focused on establishing the 6 key-objectives of the WE BUILD project, aiming to maximize value for these objectives. While doing so, the use cases were guided to carefully find the proper balance between value and feasibility. Value in terms of defining a scope as close to frequently occurring real-life situations as possible and learning as much as possible about that in relationship to the 6 key-objectives. Feasibility in terms of applying restrictions/delimitations in the pilot scope to ensure that piloting can be done respecting the (time/money/resource) constraints of the project. Real life situations were always the starting points of the exploration to find the balance between feasibility and value.

3.4 Deliverables and templates

Three templates structured the work, being:

- the Stock Taking document that was used on a use case level to identify the scenarios, partners, re-usable components, internal and external dependencies and legal frameworks.
- the scenario specification template, which had to be completed for each individual scenario. It contains process flows, challenges and barriers, working assumptions, roles and participants, attestations and requirements.
- the attestation rulebook template, used for each attestation that a use case was responsible for designing attestations, including a model of the attestation structure (an entity-relationship diagram for more complex attestations), per-object attribute definitions (name, definition, presence, data type), relevant code lists with references to applicable standards where they exist, and any integrity rules.

Using these templates for the most important ‘internal deliverables’ provided a solid base to produce the D2.1 document, the first ‘external deliverable’ of the work package.

3.5 Dependencies

WE BUILD turns out to have many dependencies between use cases, compared to previous LSPs. Several use cases use the same types of attestations, so designing and issuing attestations introduced many dependencies between many scenarios and use cases.

Collaboration across use cases was therefore a structural necessity, not an optional extra, because of the large number of shared attestations. Between ten and twenty attestation types are used by more than one use case. For each such attestation, a single use case has been assigned design responsibility. All other use cases that rely on that attestation type had to provide requirements to the responsible use case and subsequently review the resulting design. This two-way exchange — requirement handover followed by design review — is the primary mechanism for managing cross-case dependencies concerning attestation design.

The handover had to be treated as a warm, active exchange rather than a document drop. Where requirements conflict, the parties are expected to engage directly to find a resolution. There were conflicting requirements; this is anticipated, and the domain leads were available to help when conflicts could not be resolved bilaterally.

The domain leads and work package lead held biweekly check-ins with each use case lead, providing a regular forum for discussing progress, flagging issues, and seeking guidance. Beyond these scheduled touchpoints, use case leads were actively encouraged not to wait: questions, doubts, and emerging problems should be raised as they arise.

A set of cross-cutting workshops was organised for topics that affect multiple use cases, such as mandate-related attestations, tax-related attestations, digital business wallet architecture, and the structure of the EBWOID. Especially on the aspect of representation and mandates, much alignment was organized trying to find a solution that could support the needs of all different use cases. It became clear that many different perspectives existed. Use cases were asked to concentrate their energy on their own work and let the work-package leadership handle these cross-cutting topics, while remaining available when their input is needed.

Over the course of two days in an on-site event in Amsterdam, over 100 experts worked in structured workshops to produce concrete decisions on trust, identity, mandates, digital business wallets and protocols. These decisions now form the reference for implementation.

Issuance is a country-specific activity: a use case covers issuance only for the countries whose partners are part of that use case. Other use cases requiring the same attestation type for other countries must ensure their own issuance arrangements. A living mapping document tracked which use case is responsible for which attestation design and which other use cases consume the same type; this document is versioned and updated as discussions (for example, on tax-related or mandate-related attestations) produce resolutions.

Additionally, mappings were used to keep track of which use case would issue which attestation for which countries, taking into account the first mapping stating which use case uses which type of attestation. With in total roughly 40 attestations and over 20 involved countries, maintaining these mappings was an intense but necessary effort.

3.6 Roles and responsibilities

Use case leads and co-leads carried primary ownership and drove the work. They were responsible for initiating and managing the development of the pilot process descriptions, organising workshops (including on-site workshops where possible, for which use cases were explicitly encouraged to do so), coordinating within their partner group, and ensuring that the full team is assembled and documented. Domain leads and the work package lead were present to provide guidance, review interim outputs, resolve escalated issues, and facilitate cross-cutting discussions, assigned design responsibilities on attestations, monitored cross-UC consistency on processes and attestations.

Within each use case or scenario, a core team typically emerged — a smaller, more active group who do the bulk of the work, supported by a broader group whose role is primarily reviewing and contributing comments. This is a phenomenon seen more often in LSPs. What was not acceptable was complete inactivity from beneficiary partners: the first internal reporting period asked all beneficiaries to account for their hours and contributions, and persistently inactive partners would eventually be asked to exit the project, with their budget potentially redistributed.

3.7 Evaluation strategy

The use cases have finalised the learning goals on a use case level, making sure that these are again strongly related to the 6 WE BUILD key objectives as stated in the Grant Agreement. For each learning goal, an approach was designed to evaluate the project activities on several moments during the project, to secure information collection on the learning goals at the time this comes available. The strategy will be deployed throughout the remainder of the project, while the results will be the basis for the final deliverable of the works package.

3.8 Collaboration with other work packages

For Work Package 4 engagement, each use case is assigned a use case sync lead — a single point of contact within WP4's architecture group who coordinates all queries and involvement from WP4 sub-groups (wallet providers, PID/EBWID providers, QTSPs, semantics group, etc.).

To encourage collaboration across work packages even further, every use case organized at least one multidisciplinary workshop in which the use case did a structured walkthrough of a scenario and discussed challenges with experts from WP2 and WP4 to secure feasibility of the scenario as well as increased awareness with WP4 about the needs of the use case.

For Work Package 5 (business cases, governance, member state advisory board) and Work Package 6 (communication and dissemination), alignment primarily happened on work package lead level to avoid disrupting use case teams at inopportune moments. WP2 and WP5 did alignment on the establishment of so-called interest groups.

4. Overview of use cases

This chapter describes the use cases existing in work package 2, targeting the business and the supply chain domain. Each use case will be described on a high level, explaining the core of the use case. Also, the most important properties of each scenario will be explained, while a more detailed document containing process flows, specific challenges and research ambitions is available as an Annex.

In the Annex, separate scenario descriptions will be available for use cases where in Chapter 4, descriptions were merged.

4.1 Business domain

4.1.1 Use case BU1 - Know your business partner (supplier/customer/employee)

BU1 pilots the digitalisation of Know Your Business Partner (KYBP) due diligence, covering both Know Your Customer (KYC), Know Your Supplier (KYS) and Know Your Employee (KYE) processes, through the use of the European Business Wallet (EBW) as the central mechanism. The use case demonstrates a secure and fully digital cross-border onboarding process based on verifiable credentials.

In this context, an economic operator (as defined in the EBW proposal COM(2025) 838, in WE BUILD explicitly including sole traders). is enabled to prove its identity and key attributes, such as EU Company Certificate (EUCC) and VAT ID, through verifiable attestations stored in its EBW. A relying party can request, verify and process these attestations via a secure and interoperable exchange flow based on OID4VP. This allows onboarding procedures to be automated, with data reused across transactions rather than repeatedly collected through manual processes.

At its core, BU1 replaces fragmented and paper-based KYC/KYS procedures. The EBW relies on verifiable organisational identities (e.g. EBWVOID/LPID), standardised attestations (including EUCC, VAT, ownership and IBAN), and trusted cross-border verification mechanisms established through a harmonised trust framework. Together, these elements create a reusable and machine-verifiable digital identity layer for businesses.

The relevance of BU1 is both economic and regulatory. It contributes to reducing onboarding time and administrative costs for companies, facilitates faster establishment of cross-border business relationships, and decreases fraud and compliance risks, while enhancing trust and transparency within the Single Market.

BU1 constitutes a foundational building block for other use cases, as it establishes the initial identity and onboarding layer required prior to any transaction. Several use cases depend on its completion, including:

- Payments use cases (PA3/PA4), which require KYC prior to account opening or transaction execution;
- Supply chain and data space use cases (SC1/SC2), which depend on verified business identities;
- Representation use cases (BU4), which require clear identification of acting persons;

The use case is designed for pre-production piloting, while maintaining a clear pathway towards production deployment. The MVP phase foresees controlled environments with EBW-based exchanges and a limited set of attestations. Subsequent MVP+ phases expand the scope with additional credentials such as IBAN, ESG indicators or DUNS identifiers.

Different scenario's in BU1 incorporate varying assumptions and design choices, notably regarding:

- The use of EBW-only versus hybrid wallet approaches;
- The distinction between legal persons and natural persons acting in a business capacity;
- The implementation of full KYC/KYS procedures versus lighter onboarding flows;
- The composition of attestation sets used in each scenario.

The use case was decomposed into the following scenarios. Per scenario, a detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	KYC
Description	A company (Company A, country A) wants to enter into a business relationship with another company (Company B, country B) and become its customer. A legal representative of Company A initiates the onboarding by requesting and presenting required KYC attestations via a digital wallet.
Setting	Remote interaction only. The onboarding is performed via digital channels (e.g. service provider website + digital wallet interaction). No proximity (face-to-face) interaction and no machine-to-machine flow are included in this scenario.
Wallet types used	EBW
Attestations used	MVP: EBWID, EUCC, Tax number, VAT, Contact person, Ownership list, Control list, Company Info
Countries involved	DE, NL, CH, AT, FR, IT, ES
Number of relying parties	6 relying parties: La Poste, Deutsche Bahn, Orange, Bosch, Voestalpine, DFØ

Table 1: BU1 - Scenario 1

Name	KYS
Description	A company (Company A, country A) wants to enter into a business relationship with another company (Company B, country B) and become its supplier. A legal representative of Company A initiates the onboarding by requesting and presenting required KYS attestations via a digital business wallet.
Setting	Remote interaction only. The onboarding is performed via digital channels (e.g. service provider website + digital wallet interaction). No proximity (face-to-face) interaction and no machine-to-machine flow are included in this scenario.
Wallet types used	EBW
Attestations used	MVP: EBWID, EUCC, Tax number, VAT, Company information, Contact person, Ownership list, Control list, PaymentTerms, IBAN-OV Attestation

Countries involved	DE, NL, FR, AT, CH, NO, IT
Number of relying parties	7 relying parties: La Post, Orange, Robert Bosch GmbH, SBB – Swiss Federal Railways, Deutsche Bahn Cargo AG, Voestalpine Rail Technology GmbH, DFØ

Table 2: BU1 - Scenario 2

Name	KYC sole traders
Description	A sole trader (natural person acting as a business) in country A wants to enter into a business relationship with a company in country B and become its customer. The sole trader initiates the issuance and presentation of KYC attestations via a digital wallet.
Setting	Remote interaction only. The onboarding is performed digitally via digital wallet-based interaction between the sole trader and the relying party. No proximity interaction and no machine-to-machine flow are included.
Wallet types used	Hybrid setup: • EUDI Wallet (for PID, natural person identity) • European Business Wallet (EBW) optional / combined
Attestations used	MVP: PID, EUCC , Power of Representation (PoR), VAT ID, EBWVOID
Countries involved	As several relying parties, such as Google, Adyen and Deutsche Bank have establishments and customers/end users in multiple EU countries, this makes the scenario's flexible. Next to that, DE, ES, FI, FR, IT, NL, NO, PL, PT, SE are involved.
Number of relying parties	6 relying parties: Google, ComplianceWise, Deutsche Bank, Docaposte, La Poste, Adyen

Table 3: BU1 - Scenario 3

Name	KYS sole traders
Description	A sole trader (natural person acting as a business) in country A wants to enter into a business relationship with a company in country B and become its supplier. The sole trader initiates the issuance and presentation of KYS attestations.
Setting	Remote interaction only. The onboarding is performed digitally via digital wallet-based interaction between the sole trader and the relying party. No proximity interaction and no machine-to-machine flow are included.
Wallet types used	Hybrid setup: • EUDI Wallet (for PID, natural person identity) • European Business Wallet (EBW) optional / combined
Attestations used	MVP: PID, EUCC (where applicable), Power of Representation (PoR), VAT ID, Business License, Certificate of Tax Residence, EBWVOID
Countries involved	As several relying parties, such as Google, Adyen and Deutsche Bank have establishments and customers/end users in multiple EU countries, this makes the scenario's flexible. Next to that, DE, ES, FI, FR, IT, NL, NO, PL, PT, SE are involved.
Number of relying parties	6 relying parties: Google, ComplianceWise, Deutsche Bank, Docaposte, La Poste, Adyen

Table 4: BU1 - Scenario 4

Name	KYE
Description	A company (Company A, country A) sends an employee to provide services at another company (Company B, country B). The employee and/or employer presents required attestations (e.g. employee status, A1, PWN) to prove compliance with labour, social security, and cross-border service regulations.
Setting	On-site verification (e.g. inspection authorities scanning QR codes and verifying credentials face-to-face).
Wallet types used	EBW
Attestations used	MVP: PID, EBWID, EUCC, Employee Credential, A1 certificate, Posted Worker Notification (PWN)
Countries involved	DE, ES, NL, FI
Number of relying parties	4 relying parties: SICPA, DRV Bund, Bosch, Fragomen

Table 5: BU1 - Scenario 5

BU1 aims to digitalise KYC/KYS onboarding processes for businesses and sole traders in Europe using the European Business Wallet (EBW) and, where relevant, the EUDI wallet. MVP+ scenarios introduce additional data elements and more complex flows, such as IBAN data, regulatory or compliance attributes (e.g. ESG), and additional identifiers (e.g. LEI, DUNS). These scenario's will only be implemented if time and feasibility allow.

4.1.2 Use case BU2 – Piloting Company Law Directive for Company Branch Creation

The core of the BU2 use case is the fully digital, cross-border registration of a company branch in another EU Member State, enabled by the EBW. The process centres on a natural person acting on behalf of a legal entity through a digital wallet, presenting verifiable attestation to a host Member State business register, which acts as the relying party. The objective is to enable the completion of a fully online, end-to-end registration procedure without the need for physical presence or paper-based documentation.

This use case addresses a well-documented friction point in the EU internal market. Cross-border company expansion remains fragmented, administratively burdensome, and subject to divergent national procedures. By leveraging interoperable digital attestations and digital wallet technologies, the use case demonstrates how manual, repetitive, and document-intensive processes can be replaced with streamlined digital interactions. This aligns with broader EU policy objectives, including the digitalisation of company law procedures and the implementation of the “once-only” principle. Consequently, the use case directly contributes to reducing administrative burdens, enhancing legal certainty and trust in cross-border contexts, and facilitating more efficient business expansion within the EU.

The use case makes a substantial contribution to the WE BUILD objectives in several respects. First, it demonstrates the feasibility of an end-to-end, digital wallet-enabled business process, encompassing authentication, attestation exchange, and electronic signature. Second, it advances interoperability and cross-border trust by testing the exchange of attestations across jurisdictions, the validation of issuers within trust frameworks, and the technical interoperability between digital wallets and business registers.

In this context, dependencies on other use cases are critical:

- BU4 (Company representation): provides the EU PoA and related representation attestations required to verify that a natural person is authorised to act on behalf of the company. This constitutes a fundamental dependency, as the registration process cannot be executed without validated representation rights.
- BU3 (Foreign tax declaration): supports post-registration steps, such as VAT-ID issuance (VAT-registration is done in BU2), thereby enabling the branch to start business operations in the other country. This represents a strong dependency for completing the broader business lifecycle.

From an implementation perspective, the use case is positioned at a pre-production stage. It is executed within a closed pilot environment, reflecting the current legal, technical, and organisational constraints. These include the complexity and heterogeneity of national legal frameworks, the ongoing development of key standards (such as the EU PoA and elements of wallet regulation). The use of test data further underlines its focus on feasibility assessment and validation rather than operational deployment.

The use case was decomposed into the following scenarios. Per scenario, a detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	Create a company branch in an EU or EEA Member State
Description	A company established in one EU/EEA Member State applies to register a branch in another Member State. A natural person acting on behalf of the company uses an EUDI Wallet to present the required attestations to the host country Business Register, which acts as the relying party. The purpose is to support a fully digital, cross-border branch registration process.
Setting	The scenario is carried out through the eService of the host country Business Register. The flow foresees online digital wallet interactions, including same-device website-to-app and potentially cross-device QR flows.
Wallet types used	EUDI Personal Wallet and European Business Wallet. The natural person uses a personal wallet to present PID and representation-related attestations, while the Business Register uses a digital Business Wallet as relying party. The company may also hold certain attestations, such as the EUCC and/or EU PoA, in its digital Business Wallet.
Attestations used	EUCC, EU PoA, Certificate of tax residence, VAT ID, PID, EBWID
Countries involved	NO, ES, SE, FR, NL, FI
Number of relying parties	6 relying parties: BRC, Notariado, Bolagsverket/Skatteverket, Infogreffe, KvK, VERO/PRH

Table 6: BU2 - Scenario 1

Name	Registration of a company branch with a Tax Authority
Description	A company that has established a branch in another EU/EEA Member State registers this branch with the host country Tax Authority. A natural person acting on behalf of the company uses an EUDI Wallet to present required attestations (e.g. PID, EUCC, EU PoA) to the Tax Authority, which acts as the

	relying party. The goal is to complete tax registration (e.g. obtain a VAT certificate) to enable business operations.
Setting	The process is carried out via the Tax Authority's eService using digital wallet-based authentication and attestation exchange, including same-device and QR-based flows.
Wallet types used	EUDI Personal Wallet and European Business Wallet. The natural person uses the personal digital wallet to present identity and representation attestations, while the Tax Authority uses a digital Business Wallet as relying party. The company may also store attestations (e.g. EUCC, EU PoA) in a digital Business Wallet.
Attestations used	EUCC, EU PoA, Certificate of tax residence, VAT ID, PID, EBWID
Countries involved	SE, FI
Number of relying parties	2 relying parties: Skatteverket, Vero

Table 7: BU2 - Scenario 2

The BU2 "Create Company Branch" use case demonstrates how a company can first establish a branch in another EU/EEA Member State and subsequently complete its tax registration, using EUDI and digital Business Wallets to enable a fully digital, cross-border process based on verifiable attestations.

Additional MVP+ scenarios include issuance of attestations by the authentic sources and QERDS-based notifications. They may be implemented later in the project if the core MVP scenarios are successfully delivered.

4.1.3 Use case BU3 – Foreign tax declaration

The BU3 use case addresses the digitalisation of cross-border tax interactions through digital wallet-based solutions, covering processes such as VAT declaration submission and VAT ID certificate issuance. BU3 encompasses two complementary interaction paradigms:

- A portal-based model, centred on human interaction and user experience
- An M2M model, focused on automation and system-to-system integration, reflecting the intended evolution towards a scalable, digital Business Wallet-driven target architecture that improves M2M integrations from domestic to a cross-border setting

Across all scenarios, the underlying logic remains consistent: a natural person or intermediary demonstrates identity and authorisation through wallets and verifiable attestations, allowing companies to securely execute tax-related procedures with tax administrations.

The use case is underpinned by a set of interrelated technical and organisational components:

- Digital EUDI wallets for natural persons (PID) and digital Business Wallets for legal entities (LPID/EBWID)
- Authorisation mechanisms, including both central registers and attestation-based approaches
- The issuance and validation of verifiable credentials, notably Qualified Electronic Attestations of Attributes (QEAA) and Public Electronic Attestations of Attributes (Pub-EAA)

From both a policy and operational perspective, BU3 is significant in that it ensures legal certainty by enabling tax administrations to verify whether an actor is duly authorised to act on behalf of a legal entity. At the same time, it supports cross-border economic activity, particularly where intermediaries operate across multiple Member States and improve service providers' ability to operate in a cross-border setting towards foreign taxes. The integration of M2M interactions further contributes to automation and scalability, in line with the broader ambitions of the emerging Business Wallet framework, while reducing manual administrative burden by limiting the need for manual verification and providing the necessary information. In this respect, the use case operationalises the concept of digital mandates and verifiable credentials within a taxation context.

BU3 contributes directly to the WE BUILD objectives by demonstrating end-to-end cross-border wallet usage, combining natural person identifiers (PID), legal person identifiers (EBWOID), and associated authorisations within a single flow. It also provides a testing environment for different authorisation models, looking at how central registers and attestation-based approaches may co-operate and differ as solutions, as well as between service-specific and generic mandates such as EU Company Certificates (EUCC) and Powers of Attorney (PoA). Moreover, it pilots the issuance and use of domain-specific attestations, such as VAT ID, TRC and authorisation credentials. In parallel, the use case advances M2M interaction capabilities by exploring scalable communication mechanisms between digital wallets and backend systems, including protocols aligned with eDelivery or similar infrastructures.

The implementation of BU3 relies on several critical dependencies, most notably BU4 for the provision of authorisation and representation models, WP4 for the delivery of the digital wallet ecosystem and supporting trust infrastructure, and Qualified Trust Service Providers (QTSPs) for the issuance and lifecycle management (including revocation) of trust services such as electronic signatures, seals, and attestations.

The use case is designed as a pre-production pilot, operating with synthetic data while maintaining conditions that closely resemble real-world deployment. This approach enables the validation of technical feasibility, interoperability, and scalability without reliance on live data.

The use case was decomposed into the following scenarios. Per scenario, a detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	Filing VAT-declaration using Tax Portal
Description	A legal representative (natural person) located in Country B files a VAT declaration at the Tax Administration in Country A on behalf of a company in Country A via a tax portal. The Tax Administration verifies identity and authorisation (via a register or attestation) receiving the VAT-declaration.
Setting	Remote, portal-based interaction (user-to-portal). The process is human-driven (natural person logs into a tax portal and submits the declaration).
Wallet types used	Personal (EUDI) wallet for the natural person (PID, authorisation evidence) and optionally a Business Wallet for organisational credentials and VAT-declaration receipts.
Attestations used	PID, EBWOID, EUCC, PoA, service-based authorisation attestation

Countries involved	NO, NL, SE, FI, ES
Number of relying parties	Tax administrations of FI, Gipuzkoa (ES), NL, NO, SE

Table 8: BU3 - Scenario 1

Name	Filing VAT-declaration using Machine to Machine interaction
Description	A digital business wallet of an intermediary company located in Country B files a VAT declaration directly to the Tax Administration system in Country A on behalf of a company in Country A through machine-to-machine (M2M) interaction. The intermediary's identity is ensured via an electronic seal and/or electronic signature, and its authorisation is verified either via a central register or an authorisation attestation.
Setting	Remote, machine-to-machine (system-to-system) interaction between digital Business Wallet and Tax Administration system. No human portal interaction in the main flow; process is automated.
Wallet types used	Primarily EBW for the intermediary and optionally for the Tax Administration. A Personal (EUDI) wallet may be used only for supporting steps (e.g. authorisation or signature by a natural person if required).
Attestations used	PID, EBWID, Service-Based Authorisation attestation
Countries involved	NL, NO, FI, ES, SE
Number of relying parties	Tax administrations of NL, NO, FI

Table 9: BU3 - Scenario 2

Name	Issuing VAT certificate using Tax Portal
Description	A legal representative (natural person) located in Country B requests a VAT ID (as a verifiable attestation) from the Tax Administration in Country A on behalf of a company in Country A via a tax portal. The Tax Administration verifies identity and authorisation (via a register or attestation) before issuing the VAT ID certificate (QEAA or Pub-EAA) to the user's digital wallet.
Setting	Remote, portal-based interaction (user-to-portal). The process is human-driven: a natural person logs into the Tax Administration portal and initiates the request.
Wallet types used	Primarily Personal (EUDI) wallet for the natural person (PID, authorisation evidence, receiving the VAT ID attestation), with possible use of Business Wallets for organisational credentials and intermediary scenarios.
Attestations used	PID, EBWID, PoA, Authorisation attestation, VAT ID certificate
Countries involved	ES, FI, NL, NO, SE
Number of relying parties	This is an issuance only scenario, preparing attestations for other use cases.

Table 10: BU3 - Scenario 3

Name	Issuing VAT- certificate using Machine to Machine interaction
Description	A digital business wallet of an intermediary company in Country B requests a VAT-ID certificate (as a verifiable attestation) from the Tax Administration in Country A on behalf of a company in Country A via machine-to-machine

	interaction. The Tax Administration verifies the identity and authorisation of the intermediary (via register or attestation) before issuing the VAT-ID certificate (QEAA or Pub-EAA) to the intermediary's digital business wallet.
Setting	Remote, machine-to-machine (system-to-system) interaction between Business Wallet and Tax Administration system. Fully automated flow, without direct human portal interaction.
Wallet types used	Primarily EBW for the intermediary and (optionally) the Tax Administration or issuer. A Personal (EUDI) wallet may be used only for supporting steps
Attestations used	PID, EBWOID, PoA, Service-based authorisation attestation, VAT ID certificate
Countries involved	NL, NO
Number of relying parties	This is an issuance only scenario, preparing attestations for other use cases.

Table 11: BU3 - Scenario 4

The BU3 use case demonstrates how cross-border tax processes (VAT declaration, VAT-ID issuance, and Tax Residency Certificate issuance) can be securely digitalised using EUDI and digital Business Wallets, enabling both portal-based (human-driven) and machine-to-machine (automated) interactions with verified identity and authorisation.

In addition to the core VAT-related scenarios (MVP), the use case also includes Tax Residency Certificate scenarios (Scenarios 5 and 6) as MVP+ stretch goals, which are not yet fully detailed due to external dependencies and limited maturity, but may be developed later in the project if time and conditions allow.

4.1.4 Use case BU4 – A company representative acting and signing on behalf of company

The core objective of BU4 is to enable a natural person, or a legally authorised proxy, to act on behalf of a legal entity in a legally valid and verifiable manner through the use of digital wallets and standardised attestations, notably Power of Authority (PoA) and Power of Representation (PoR). Scenarios 1a and 1b address the issuance of such representation credentials, while Scenario 1c focuses on their subsequent use in accessing services. Collectively, these scenarios establish a complete lifecycle encompassing the creation of representation rights through issuance, their secure storage within digital wallets, and their verification and use by relying parties.

This use case is of particular relevance given that a wide range of business processes, such as tax filing, banking services, and participation in commercial platforms, require formally authorised representation. At present, cross-border operations lack harmonised and interoperable mechanisms for digital representation, which constitutes a significant barrier within the EU digital single market. BU4 addresses this gap by enabling the reliable and cross-border verification of who is entitled to act on behalf of a company. Conceptually, the use case can be understood as an implementation of “authorisation as a service,” whereby legal mandates are transformed into machine-readable, cryptographically verifiable, and interoperable credentials.

BU4 directly supports the objectives of WE BUILD by establishing a framework for trusted digital representation, ensuring that actions performed on behalf of a legal entity are traceable,

authorised, and legally valid. It further promotes interoperability across Member States by introducing a common semantic model and taxonomy for mandates, thereby facilitating cross-border recognition and verification. In addition, the use case enables end-to-end wallet-based business processes by integrating identity credentials (PID/EBWID), company data (such as the EUCC), and mandate attestations (PoA, PoR, PoE), which together support secure and automated access to services.

Beyond its standalone value, BU4 functions as a horizontal enabler, providing the authorisation layer required for a wide range of other business use cases; without such a layer, most transactions involving representation could not be executed digitally.

Key interdependencies arise with other business use cases and technical components:

- BU1 (KYC/KYB/KYS): Provides the foundational identity and company verification prerequisites, with explicit dependencies for the completion of representation-related scenarios.
- BU2 (Creation of a company branch): Relies on clearly defined representation rights, necessitating PoA and PoR frameworks.
- BU3 (Foreign tax declaration): Depends directly on delegation and representation mechanisms, for example in the case intermediaries like tax advisors or accounting firms.
- WP4: Include digital wallet providers (EUDI/EBW), qualified trust service providers (for issuing qualified electronic attestations), PID/EBWID providers, and supporting trust infrastructure such as status and revocation services.

Finally, BU4 is positioned as a pilot use case intended to demonstrate production readiness, while remaining in a pre-production phase. It does not yet deliver fully operational production services but is explicitly designed to validate the technical, legal, and organisational conditions necessary for future large-scale deployment.

The use case was decomposed into the following scenarios. Per scenario, a detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	Issuance Powers of Attorney
Description	A natural person (for example a lawyer) uses a Business Wallet containing Power of Representation (PoR) and/or Power of Attorney (PoA) attestations to prove authorization to act on behalf of a legal entity and access digital services provided by cross-border public or private relying parties.
Setting	Remote, wallet-based interaction, including cross-border context. No proximity or M2M explicitly part of the core MVP scenario.
Wallet types used	- Business Wallet (EBW) for storing the PoA and managing mandates - EUDI Wallet (EUDIW) for identity (PID) presentation during issuance
Attestations used	PID, EBWID, PoA, PoR
Countries involved	NL, DE, ES, BE, SE, IT, GR, FR
Number of relying parties	This is primarily an issuance scenario.

Table 12: BU4 - Scenario 1a

Name	Issuance Powers of Representation
Description	This scenario pilots the issuance of a Powers of Representation (PoR) attestation to an EU Business Wallet (EBW), enabling the person, either natural or legal, to prove they are authorized to represent a company in digital interactions. The PoR attestation is issued based on information held in authentic sources, such as Business Registries, and is issued by a Qualified Trust Service Provider (QTSP) acting on behalf of an authentic source, or by a public sector body responsible for an authentic source.
Setting	Remote, digital wallet-based interaction, including cross-border context. No proximity or M2M explicitly part of the core MVP scenario.
Wallet types used	European Business Wallet is primary wallet for receiving and storing PoR)
Attestations used	EBWOID, PoR
Countries involved	AT, DE, NL, SE, ES, GR, IT,
Number of relying parties	This is primarily an issuance scenario.

Table 13: BU4 - Scenario 1b

Name	Get access to a service
Description	A natural person uses a Business Wallet or a EUDI Wallet containing Power of Representation (PoR) and/or Power of Attorney (PoA) and/or Power of Employee (PoE) attestations to prove authorization to act on behalf of a legal entity and access digital services provided by cross-border public or private relying parties.
Setting	Remote (core flow), with variations including same-device and cross-device interaction, and optional intermediary platforms; no machine-to-machine interaction in MVP scope.
Wallet types used	- EUDI Wallet (EUDIW) (primary for identity and presentation) - Business Wallet (EBW) (for storing PoA/PoR and company-related credentials)
Attestations used	PID, EBWOID, Qualified Electronic Attestation / Qualified Certificate for signature validation, Credential Status / Revocation Information, Power of X (PoX) – Representation and Mandate Attestation (PoR + PoA + scope limitation), Power of Employee (PoE) – Organizational Representation Attestation
Countries involved	AT, BE, SE, DE, GR, FR, ES, NL
Number of relying parties	6: OpenPeppol, Itsme, Skatteverket, DATEV & Telekom, GRNET, Orange and others in other use cases

Table 14: BU4 - Scenario 1c

The BU4 use case establishes a complete lifecycle for digital corporate representation by enabling the issuance (PoA/PoR) and subsequent use of verifiable mandates to access cross-border services via digital wallets, thereby operationalizing legally valid “acting on behalf of a company” in the European digital ecosystem.

In addition to the MVP scenarios above, the use case also foresees MVP+ scenarios (cross-border tax declaration, cross-border European transformation, and automated presentation)

which are treated as stretch goals due to their higher complexity and external dependencies and may be further developed later in the project if the initial pilot progresses successfully.

4.1.5 Use case BU5 – Issue micro Credentials

The BU5 use case concerns the issuance, management, and utilisation of digitally verifiable skill credentials, namely micro-credentials (and verified skills as MVP+), through the EUDI Wallet. It enables natural persons to demonstrate learning outcomes and competences in a cross-border context in a manner that is trusted, interoperable, and user-controlled. These credentials are realised as Electronic Attestations of Attributes (EAAs), which are issued by legitimate authorities, stored within the digital wallet, and presented to relying parties to support decision-making processes.

More specifically:

- Micro-credentials refer to formally assessed learning outcomes within an educational context.
- Verified skills (MVP+) denote assessed competences acquired in real-world or labour market settings.
- Both credential types are structured as EAAs, ensuring portability, authenticity, and interoperability across systems.

The use case addresses a recurring requirement in both cross-border and domestic digital interactions: enabling individuals to provide verifiable evidence of knowledge, skills, and competences with clear academic provenance. In practice, this entails the ability of a user to obtain a digitally issued attestation from a recognised issuer, store it securely in an EUDI Wallet, and present it to a relying party when required in the context of a service, administrative procedure, or eligibility assessment. The underlying trust objective extends beyond technical portability to encompass semantically consistent and organisationally reliable exchange of attributes, while preserving user control over data disclosure. BU5 is explicitly designed to ensure alignment between formal education credentials and labour market evidence, thereby bridging the gap between micro-credentials and verified skills (MVP+).

Key challenges of the use case include:

- Misalignment between existing educational data standards (e.g. ELM) and EUDI Wallet formats
- Absence of harmonised quality assurance mechanisms for non-formal and informal skills
- Limited semantic consistency across jurisdictions and sectors

The use case also demonstrates synergies at both operational and technical levels:

- With other WE BUILD use cases (SC1), particularly through the potential reuse of verified skill credentials in supply chain contexts
- With the semantic and rulebook activities under WP4, notably in the joint development of credential schemas, metadata models, and interoperability standards

Finally, the use case is positioned within a pre-production pilot context. Its objective is to refine understanding of the operational and technical implications of such a system prior to full deployment. In this respect, the pilot aims to:

- Validate technical and organisational feasibility
- Identify interoperability constraints and gaps
- Develop guidance to support future large-scale rollout

The use case was decomposed into the following scenarios. Per scenario, a detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	Micro-credentials
Description	This scenario concerns the issuance and use of digitally verifiable micro-credentials representing formally assessed learning outcomes within an educational context. Accredited issuers (e.g. universities or training providers) issue these credentials as Electronic Attestations of Attributes (EAAs), which are stored in the EUDI Wallet and can be presented by the holder to relying parties (e.g. employers or educational institutions) to support decision-making processes such as recruitment, admission, or certification recognition.
Setting	Primarily remote interactions, with potential applicability to both cross-border and domestic contexts; no strict requirement for proximity or machine-to-machine interaction, although integration with institutional systems may enable partial automation.
Wallet types used	EUDI Wallet
Attestations used	PID, micro-credential
Countries involved	SE, GR
Number of relying parties	2 relying parties: Linköping University, UAegean

Table 15: BU5 - Scenario 1

The BU5 use case addresses the issuance and use of both micro-credentials (and verified skills as MVP+) as digitally verifiable attestations within the EUDI Wallet, enabling natural persons to demonstrate formally assessed learning outcomes and real-world competences in a trusted and interoperable manner across borders and sectors.

In addition to these core scenarios, the use case foresees further MVP+ scenarios as stretch goals, such as the extended reuse of skill credentials in more complex interoperability or sector-specific contexts.

4.1.6 Use case BU6 – Business access to the Once Only Technical System (OOTS)

The core objective of BU6 is to explore and validate the integration between the European Digital Identity (EUDI) Wallet and the Once-Only Technical System (OOTS). This integration enables users, specifically natural persons acting on behalf of legal entities, to combine both channels to provide identity, representation, and company-related data to public services within a unified interaction flow.

Concretely, the use case focuses on authenticating users through the EUDI Wallet using the Person Identification Data (PID), demonstrating powers of representation (PoR), and retrieving company data via OOTS. These elements are combined into a user-controlled process that allows individuals to dynamically orchestrate how identity attributes and company information are shared with relying services.

The relevance of BU6 stems from its role in bridging a structural gap between identity ecosystems (centred around the digital wallet) and data exchange infrastructures (such as OOTS). By enabling this integration, the use case supports cross-border business interactions in line with the Single Digital Gateway framework. Furthermore, it introduces a user-centric approach that enhances flexibility, allowing users to combine wallet-based attestations with evidence retrieved through OOTS depending on the specific context of the interaction.

The use case demonstrates clear dependencies on other components of the ecosystem. In particular, it reuses attestations developed in other use cases, including powers of representation and powers of attorney (BU4), as well as company-related attestations such as the EU Company Certificate (BU2). In addition, BU6 is strongly dependent on the outcomes of WP4, as the availability of digital wallet infrastructure, including PID and EBWOID issuance and the broader trust framework, is a prerequisite for its execution.

Finally, BU6 is primarily designed to be validated within a pre-production environment, rather than targeting immediate deployment in a fully operational production context.

The use case was decomposed into the following scenarios. Per scenario, a detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	Full Power authentication for OOTS
Description	A natural person applies for a cross-border business service on behalf of a company, using the EUDI Wallet to authenticate and prove full power of representation (PoR) at both the relying party and during re-authentication in the OOTS flow. Company data are retrieved via OOTS from the relevant Member State and shared with the relying party under user consent (s part of the regular OOTS-requirements).
Setting	Remote: cross-border interaction between relying party MS and evidence provider MS through OOTS
Wallet types used	EUDI Wallet
Attestations used	PID, PoR
Countries involved	GR, PL, PT, SI, NL
Number of relying parties / intermediary	4 OOTS platforms

Table 16: BU6 - Scenario 1

Name	Fine Grained Powers authentication for OOTS
Description	A natural person applies for a cross-border business service on behalf of a company, using the EUDI Wallet to authenticate and prove fine-grained powers of representation (PoR) limited to a specific SDG service. The

	authentication and re-authentication occur both at the relying party and within the OOTS flow, while company data are retrieved via OOTS and shared under user consent.
Setting	Remote: cross-border interaction via OOTS between relying party and evidence provider Member States
Wallet types used	EUDI Wallet
Attestations used	PID, PoR
Countries involved	PL, PT, SI
Number of relying parties	3 relying parties: MRIT, GOV.PT, MDT

Table 17: BU6 - Scenario 2

The BU6 use case explores the integration of the EUDI Wallet and the OOTS to enable natural persons to authenticate, prove representation powers, and exchange company data in cross-border business services through a seamless, user-controlled flow. In addition to the MVP scenarios on full and fine-grained power authentication, three MVP+ scenarios are defined:

- issuance of attestations via OOTS
- presentation of wallet attestations through OOTS
- use of a digital Business Wallet

These scenarios can be seen as extensions to the MVP scenarios and will only be investigated at a later stage of the project, subject to progress on the MVP scenarios.

4.2 Supply Chain domain

4.2.1 Use case SC1 – Authentication and access for transport

SC1 pilots the digitalisation of authentication and access management within the transport and logistics sector, covering company onboarding, facility access control, and cross-border freight documentation processing using the European Business Wallet (EBW) and Natural Person Wallets as central mechanisms. The use case demonstrates secure, legally trusted, and fully digital workflows for cross-border transport logistics based on verifiable credentials.

In this context, transport operators and drivers are enabled to prove their identity, employment status, and consignment rights (EBWID, PID, Power of Employee (PoE), and electronic consignment notes (eCMR)¹) through verifiable attestations stored in their digital wallets. Relying parties, including Port Community Systems (PCS), Terminal Operating Systems (TOS), and public enforcement authorities, can request, verify, and process these attestations via secure exchange flows. This allows gate check-ins, contracting, and roadside compliance inspections to be automated, reducing manual verifications and paper tracking while moving goods across borders.

¹ An eCMR is the digital, electronic version of the traditional paper CMR consignment note (Convention relative au contrat de transport international de marchandises par route), which serves as the official contract of carriage for international road freight.

At its core, SC1 replaces fragmented, paper-based, and repetitive logistics identification procedures (such as physical gate badges or printed waybills). The ecosystem relies on verifiable organizational and individual identities, domain-specific logistics tokens (including cargo tokens and terminal access authorizations), and trusted query frameworks linked directly to the European electronic Freight Transport Information (eFTI) network. Together, these elements create an interoperable, machine-verifiable data layer that bridges private supply chain operations with regulatory public oversight.

The relevance of SC1 is both economic and regulatory. Mathematically and operationally, it reduces vehicle gate-access and cross-border check times significantly. It accelerates data exchange between heterogeneous IT systems, cuts compliance and administrative overhead for carriers, ensures strict alignment with EU maritime security (ISPS Code) and transport rules (eFTI Regulation), and substantially decreases documentation fraud in the Single Market.

SC1 builds upon the identity layers established by other foundational initiatives and WP4, requiring verified enterprise and personal datasets prior to completing logistical transactions. The execution of its scenarios depends on or closely interfaces with several components, including:

- Know Your Business partner (BU1), which provides the initial enterprise identity layer (EBWID/EUCC);
- Foreign Tax Declaration (BU3), which delivers required enterprise tax attributes (such as VAT ID certificates) at the onboarding phase;
- Representation use cases (BU4), which outline the specifications for powers of attorney and employee mandates;
- eInvoicing (SC5), which designed the Peppol ID attestation for SC1 use case captured during the initial carrier enrolment to be used as a business identifier and facilitate automated eInvoicing according to the requirements of PCS.

The use case is designed for pre-production piloting, maintaining a clear pathway towards production deployment within critical transport infrastructure. The MVP phase foresees controlled environments validating company enrolment to ports, secure terminal access checks, and a baseline eCMR lifecycle managed through a single platform. Subsequent MVP+ phases expand the scope to cross-border Gate-to-Gate queries over the eFTI network, advanced/qualified electronic seals (QES), and extended logistics attributes like EORI and Peppol identifier.

Different scenarios in SC1 incorporate varying assumptions and design choices, notably regarding:

- The use of natural person wallets versus business and professional wallet variants, for example a mobile client for the enterprise employee to act through an attestation issued by the organisation that proves identity and representation, with defined powers and having that attestation delivered either through the person's own digital wallet client or a mobile client.

- The proximity (offline-capable) versus remote data exchange flows required for roadside or maritime terminal checks;
- The integration of intermediary verification platforms to abstract infrastructure complexity for relying parties;
- The coordination between private commercial business flows and public authority enforcement queries.

The use case includes the following scenarios. Per scenario, a detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	Enrolment and trusted contracting
Description	A transport company is onboarded to a Port Community System (PCS). The company completes KYB procedure on the PCS portal. KYB attestations are issued to the natural person wallet if sole trader (EBWOID, EUCC), or to the business wallet otherwise (EBWOID, EUCC). VAT ID is issued by the tax authority of the country issued the EBWOID. Legal representative registers the company to the PCS services and signs contract. Employee is mandated to use the business wallet for SSO on PCS. The PCS Provider uses an intermediary for verification of attestations.
Setting	Access to the eService of PCS portal. Mandate management functionality in the EBW
Wallet types used	EUDI, EBW, mobile client of the EBW for the enterprise employee
Attestations used	MVP: EBWOID, PID, EUCC, VAT ID, Employee Attestation (PoE), UBO
Countries involved	NL, FR, DE, ES, BE (TBC), PL (TBC)
Number of relying parties	2 Relying Parties: Portbase NL, Portic ES (TBC)

Table 18: SC1 -Scenario 1.1

Name	Identify and security access
Description	Driver, and carrier company are identified for secure physical terminal gate access. The company of the driver has a valid EBW with its EBWOID. A PoE is issued for the specific driver that is going to pick up the cargo from the port. The PCS checks the driver's company and PoE at the time of accessing the terminal for picking up the cargo. Other checks done at the very same time, like Transport permit, Driver license, Safety instructions, Dangerous goods certificate etc. are out of the scope of the scenario. The pilot focuses on road transport and maritime/inland port operations and EU cross-border scenarios only.
Setting	Proximity with offline capability
Wallet types used	EUDI, EBW, mobile client of the EBW for the enterprise employee with the attestation issued by the organisation that proves identity and representation, with defined powers
Attestations used	MVP: EBWOID, Employee Attestation (PoE)
Countries involved	NL, FR, ES, DE, BE, PL

Number of relying parties	2 Relying Parties: Secure Logistics + Rotterdam ShortSea Terminals NL Portic + [Port authority/terminal collaboration] ES (TBC)
---------------------------	---

Table 19: SC1 – Scenario 1.2

Name	eCMR/eFTI compliant cross-border transport
Description	At pickup and delivery of the goods, every company involved (shipper, carrier, consignee) are identified with a valid EBWOID and a EBW by the eCMR/eFTI platform that is managing the entire eCMR lifecycle. The eCMR attestation issued to a company and presented by the driver with its EBW is a multi-purposes attestation: • Link to eCMR, used to give access only to the right consignment data; • The document itself for offline presentation by the driver (PDF); • eFTI QR Code for roadside checks by authorities (via eFTI network).
Setting	Access to eService of eCMR/eFTI platforms, proximity and offline capabilities
Wallet types used	EBW
Attestations used	EBWOID, PID, EUCC, PoR, eCMR
Countries involved	BE, DE, EE, ES, FR, NL
Number of relying parties	NL, EE, ES, FR (TBC) Consignment issuers / eCMR / eFTI Platform operators: Pionira (BE), Ybil OU (EE), Fieldeas (ES), CEVA (FR, tbc)

Table 20: SC1 - Scenario 1.3

SC1 shifts transport and logistics into a fully digital paradigm by anchoring company onboarding, facility access, and cross-border freight documentation within the European Business Wallet and Natural Person Wallets.

Additional MVP+ scenarios will be explored including advanced/qualified electronic seals (QES) for trusted contracting, additional attestations like LEI, IBAN, UBO, EORI, and Peppol ID to ease identification and eInvoicing, and eFTI QR code to be used at border or checkpoint controls. These scenarios will only be implemented if time and feasibility allow.

4.2.2 Use case SC2 – Trusted data sharing for dataspace

SC2 pilots the digitalisation of secure, cross-border onboarding and verification processes for Legal Persons across multiple Data Space Initiatives (DSIs), utilizing the European Business Wallet (EBW) as the central mechanism. The use case demonstrates an interoperable, wallet-based ecosystem where organizations can seamlessly establish their identities and manage trusted data relationships within a controlled 'mini' dataspace environment—specifically piloted under the name "Agri-X" consisting of three DSIs - DjustConnect, DIH Agrifood Data Space (DADS) and Tritom and serves as a pilot towards broader Data Space adoption (e.g. CEADS, SAGE, Catena-X, etc).

In this context, an economic operator is enabled to prove its organizational identity and platform relationships through verifiable business-level attestations, such as the EBWOID, VAT ID, and a newly introduced Dataspace Membership Credential stored within its EBW. Relying parties, consisting of participating digital data platforms, can request, verify, and process these attestations to determine if a company aligns with required (dataspace) governance standards

and conditions. This allows onboarding procedures across different sectoral or regional data platforms to be automated, allowing businesses to reuse their credentials across transactions rather than repeatedly completing manual and fragmented registration procedures.

At its core, SC2 replaces traditional, isolated platform registration workflows with an integrated, machine-verifiable trust layer. The EBW architecture leverages authoritative identifiers, standardized attestation models (such as the W3C Verifiable Credential Data Model supporting JSON-LD and SD-JWT formats), and shared data space governance structures. Together, these elements enable a Membership Credential issued by one platform to show other ecosystem participants which data platform an organization is securely sharing data with or consuming data from, completely decoupling identity verification from the underlying data transfer technology.

The relevance of SC2 is both economic and regulatory. It dramatically reduces administrative friction and time-to-onboard for smaller economic actors (such as farmers and SMEs), simplifies cross-border data collaborations within the single market, and establishes a clear trust architecture that aligns with evolving European digital standards like the eIDAS 2.0 framework and Data Space Support Centre (DSSC) blueprints.

SC2 builds upon foundational digital blocks and interacts with other broader enterprise identity layers. Several prior capabilities and dependencies influence or run parallel to its successful execution, including:

- Know Your Business partner (BU1), which provides the critical design inspiration for enterprise wallet onboarding and establishes compatibility with future high-assurance artifacts like the European Company Certificate (EUCC) to be supported in the future;
- Foreign Tax Declaration (BU3), which drives the underlying design and validation rules for checking required fiscal credentials like the VAT ID that can be used for identification and authentication of an economic operator.

The use case is designed for pre-production piloting, while maintaining a clear pathway towards production deployment within live cross-border environments. The MVP phase foresees system testing within a controlled environment involving three specific digital platforms – DjustConnect (Belgium), DIH Agrifood Data Space (Slovenia), and Tritom (Finland) – using a primary focus on JSON-LD format and mocked foundational identity attributes as the Business Registries related to the member states of 2 DSIs (Belgium and Slovenia) are not represented in the use case. Subsequent MVP+ phases expand the scope to explore a formal data space Trust Framework, natural person representations, mandates, delegation structures, and the use of specialized data usage licenses. SC2 incorporates specific assumptions and design choices, notably regarding:

- The format for semantic interoperability; the primary format is JSON-LD due to the importance of the JSON-LD format within the dataspace domain and its semantic interoperability. However, as the focus of most wallet providers is SD-JWT as well as there is no guarantee that business registries will eventually issue VAT-ID in the JSON-LD format, the pilot is considering piloting both credential formats in a phased approach.

- The validation requirements separating standard new-user onboarding from shortened outbound credential issuance paths tailored for members that are already on-boarded via a non-wallet way, but they can adopt the membership credential to use it for accessing other DSIs;

The use case includes the following MVP scenario. A detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	Onboarding CEADS (Common European Agricultural Data Space)
Description	A Legal Person (including one-person companies acting as legal entities) onboards at one DSI A by accepting the governance rulebook of the DSI. It receives a Membership credential specific to the DSI and this credential is stored in the European Business Wallet. This credential can then be presented to another DSI (DSI B), which can verify it and allow onboarding without requiring full re-registration in case dataspace governance rulebooks are compliant or accepted before.
Setting	Remote, wallet-based interaction, including cross-border context.
Wallet types used	European Business Wallet. The company may also store attestations (e.g. EUCC, EU PoA) in a Business Wallet.
Attestations used	EBWOID, VAT ID, Dataspace membership credential
Countries involved	BE, FI, SI
Number of relying parties	3 relying parties: ILVO – DjustConnect platform BE, Dataspace Europe – Tritom platform FI, ITC – DADS platform SI,

Table 21: SC2 - Scenario 1

SC2 aims to digitalise seamless onboarding processes across Data Space Initiatives in Europe using the European Business Wallet (EBW) and the verifiable membership credential.

Additional MVP+ scenarios will be explored including an additional (dataspace) trust layer added via a (dataspace) Trust Framework, mandates and delegation, and data usage licenses. These scenarios will only be implemented if time and feasibility allow.

4.2.3 Use case SC5 - eInvoicing

SC5 pilots focus on using the European Business Wallet (EBW) for enhancing trust in electronic invoicing (eInvoicing) processes across the European Single Market, both within the Peppol Network and in other invoice transmission mechanisms (such as direct wallet-to-wallet eInvoicing scenario). The use case aims to demonstrate the feasibility and value of secure, legally trusted, and fully digital and automated business-to-business (B2B) and business-to-government (B2G) eInvoicing workflows based on verifiable credentials.

In this context, an economic operator is enabled to prove its trusted contractual relationships, and service provider mandates through verifiable attestations—such as the Approved Supplier attestation, and Authorized Service Provider attestation—stored within their digital business wallets. Relying parties, including corporate buyers, network Access Points (APs), and national Tax Authorities, can request, verify, and process these attestations via secure, interoperable exchange flows based on standard protocols like OpenID4VP and OpenID4VCI.

At its core, SC5 addresses traditional eInvoicing risks (such as invoice fraud, unauthorized invoice submission) by introducing a standardised, and interoperable layer of machine-verifiable trust. The EBW architecture relies on verifiable organizational identities (EBVOID) and harmonized cross-border verification mechanisms. Together, these elements overlay a secure, cryptographic authentication and authorisation framework onto established transport networks like Peppol, without forcing intrusive changes to the underlying message formats or transport infrastructure protocols.

The relevance of SC5 is both economic and regulatory. It significantly reduces administrative overhead and processing costs for trust establishment, reduces the need for manual and bespoke systems applying business controls to invoice flows and facilitates cross-border interoperability. Furthermore, it aligns businesses directly with other upcoming European regulatory frameworks, notably the VAT in the Digital Age (ViDA) initiative, which mandates real-time or near-real-time reporting of intra-community transactions to tax administrations using eInvoicing data.

SC5 builds upon the foundational identity layers established in WP4 and preceding business onboarding flows, as studied within use cases such as:

- Know Your Business partner (BU1), which provides the initial enterprise identity, KYC/KYS onboarding step, and baseline attestations needed before invoicing procedures are triggered;
- Representation use cases (BU4), which determine the specifications for underlying organizational mandates and acting personnel identities.

The SC5 use case is designed for pre-production piloting, while maintaining a clear pathway towards production deployment in current eInvoicing exchanges. The MVP phase foresees automated system-to-system exchanges in controlled environments executing supplier pre-approval workflows, service provider authorisation, and direct wallet-to-wallet invoicing using a limited set of core credentials (such as SD-JWT VC formats). Subsequent MVP+ phases expand the scope to integrate Tax Authority verification of service provider authorisation to submit data on behalf of taxpayers under the ViDA reporting compliance and advanced electronic registered delivery services (ERDS/QERDS).

Different scenarios in SC5 incorporate varying assumptions and design choices, notably regarding:

- The use of standard network-intermediated distribution models (Peppol 4-corner architecture) versus direct, peer-to-peer wallet-to-wallet transfer protocols;
- The implementation of pre-transmission validation handshakes versus embedding cryptographic trust components directly into data flows;
- The choice of transport semantic layers, balancing low-complexity OpenID4VP/DCQL protocol structures against the legally robust qualified electronic delivery (QERDS) pathways.

The SC5 use case includes the following scenarios. They share a common foundation where applicable. Scenarios 1, 2, 3 and 5 are built on the Peppol network's 4-corner model, enhanced

with EBW attestations to strengthen trust and enable machine-verifiable authorization. Scenario 4 uses the "reference attestation" concept to enable the Buyer's Business Wallet validate authenticity and integrity of the eInvoice, independent on transfer mechanism. Per scenario, a detailed design including process flows, assumptions, scoping decisions and involved partners is available as an Annex, as are rulebooks for the attestations to use.

Name	Supplier pre-approval
Description	A legal person acting as a buyer with its EBW issues an Approved Supplier credential to the EBW of a legal person acting as a Supplier proving the existence of a trusted and acknowledged business relationship between the two parties and therefore confirms that the supplier is acknowledged and trusted to send eInvoices to the specific buyer. The Supplier stores this attestation in its EBW and presents it when sending an invoice. The Service Provider verifies the attestation before routing or accepting the eInvoice.
Setting	Machine to machine
Wallet types used	EBW
Attestations used	Approved Supplier attestation as an EAA, EBWOID
Countries involved	As several Service Providers acting as relying parties, such as B2BRouter, ILYDA, DATEV, Banqup, Ledger Leopard have customers/end users in multiple EU countries, this makes the scenario flexible. Countries involved FR, BE, NL, DE, GR, ES, SE.
Number of relying parties	5 Relying Parties: B2BRouter, ILYDA, Banqup, Ledger Leopard, Datev

Table 22: SC5 - Scenario 1

Name	Service Provider authorization
Description	A legal person acting as a buyer or a supplier with its EBW issues an Authorised Service Provider credential to the EBW of a legal person acting as its Service Provider (SP) proving that the SP is authorised to act on the company's behalf for one or more explicitly defined functions, including sending or receiving electronic invoices on its behalf, and submitting VAT or transaction data to tax authorities. The Service Provider holds and presents this attestation during eInvoicing exchanges, while the business partner's Service Provider verifies it before accepting and processing the invoice, ensuring that only invoices sent by authorized intermediaries are trusted and processed.
Setting	Machine to machine
Wallet types used	EBW
Attestations used	Authorised Supplier Attestation as an EAA, EBWOID, EUCC
Countries involved	As several Service Providers acting as relying parties, such as B2BRouter, ILYDA, DATEV, Banqup, Ledger Leopard have customers/end users in multiple EU countries, this makes the scenario flexible. Countries involved FR, BE, NL, DE, GR, ES, SE.

Number of relying parties	6 Relying Parties B2BRouter, ILYDA, GSIS, Banqup, Ledger Leopard, Datev
---------------------------	---

Table 23: SC5 - Scenario 2

Name	Direct eInvoicing between Business Wallets
Description	A legal person acting as Supplier issues an eInvoice Attestation and delivers it using their Business Wallet directly to a Buyer Business Wallet, which verifies invoice integrity, supplier identity, and authorization. The eInvoice Attestation used is a verifiable representation (linked attestation) of an invoice exchange event, binding invoice content (via a payload hash) to a cryptographic signature associated with the Supplier's legal-person identity.
Setting	Machine to machine
Wallet types used	EBW
Attestations used	eInvoice attestation, EBWOID, EUCC
Countries involved	DE, NL
Number of relying parties	1: Bosch

Table 24: SC5 - Scenario 4

SC5 aims to enhance the trust of eInvoice exchange transactions over the Peppol network or other transmission mechanisms using the European Business Wallet (EBW) enabling authorised invoice submissions by verification of existing supplier-buyer relationships and allowing receivers to only receive invoices from authorised suppliers via authorised service providers in the case of the Peppol network.

Additional MVP+ scenarios will be explored including Service Provider authorization verifiable by Tax Administration which extends the Authorized Service Provider attestation from Scenario 2 to the tax reporting context under ViDA (VAT in the Digital Age) and additional or alternative trust-building mechanism that can be introduced into the standard Peppol flow, beyond the attestation-based approach of Scenarios 1 and 2. These scenarios will only be implemented if time and feasibility allow.

5. Scoping decisions and working assumptions

5.1 Scoping decisions

The final scope of the use cases and scenarios was created and agreed upon by the partners actually involved in these use cases / scenarios, keeping the interest of real-life citizens, business and other stakeholders in mind, as was the intentions in the Grant Agreement. The involvement and the capabilities of the partners greatly influenced the feasibility and the ambition of what can and will be piloted in the work package.

The use cases applied the following directives were used to design the pilots.

- In general, all use cases were assigned to focus on the core of the use cases and pay less attention to all kinds of exceptions and technical errors that could happen during the process. This is because WE BUILD is targeting learnings on value in processes in different industries, create best practices and provide feedback to the ARF and Implementing Acts.

- In line with the Grant Agreement key-objectives and use case descriptions, the use cases focused on learning about the value, feasibility and process-complexity if using the digital (business) wallet in several different industries and situations.

The key-objectives (test-out, provide recommendations, build a foundation for the EBW, re-use from previous LSPs, increase infrastructure maturity towards large scale adoption, connect with other European infrastructures) were the main guidelines for detailing the use cases and their scenarios. Other topics like data-protection were (not disqualifying its importance) of secondary concern and (only) addressed after addressing the primary objectives was achieved.

Privacy challenges related to use cases involving the EBW remain under observation and may require further clarification as the legal framework continues to evolve. This assessment may extend beyond the duration of WE BUILD, particularly until a consolidated legal framework has been established.

- For attestation formats the use cases will start with SD-JWT and mdoc (if needed). For the attestations, rulebooks are produced to define the understanding of all attributes and structures of attestations, ensuring the interoperability in the ecosystem. The use cases produced attestation descriptions and rulebooks in a version 1.0, allowing implementation to start. Version 2.0 is expected early in the implementation phase of the project, bringing semantic improvements but not changing the structures and nature of the attestations. One use case (Supply Chain 2) immediately starts with the JSON-LD format because the industry that the use case is active in, uses that format already. Time permitting, other use cases may explore this format later in the project if time permits.
- In LSPs a tension exists between solutions being fully ready for real-world-usage, covering all complexity and all exceptions that may exist, and solutions that are feasible and good enough for piloting. Feasibility is greatly determined by the amount of time and resources available, but also by the number and expertise of the involved partners. The use cases tried to find the sweet spot in this balance, and from there stretch the ambition slightly towards the 'real-world' solution. Usage of 'fit4pilot' catalogues for mandates is an example of reducing complexity to increase pilot feasibility.

This means that much will be covered and learned for future full-scales roll-out of the digital wallet ecosystem into the real world, but in some areas additional enhancements may need to be applied to make solutions ‘real-world-proof’.

5.2 Main working assumptions

Many working assumptions were made in the use cases. Some very specific for a single use case, while others seemed to be more generic. This section covers the main and generic working assumptions applied in the use cases.

Next to the main working assumptions, WE BUILD works with so-called Architecture Decision Records. These are not included in the list below.

- Synthetic data

The use cases will primarily be piloting in pre-production using synthetic data. The use of synthetic data is expected to significantly reduce privacy risks and limit the applicability of the GDPR to complex data processing activities. Consequently, the primary safeguards anticipated to apply, as described in D1.4-Data Protection & Ethics and further elaborated in the WE BUILD Piloting Guidelines, are those relating to the voluntary and informed involvement of human participants.

Piloting in production is however not excluded by default: for use cases that mature fast and for which conditions can be established to pilot in a production environment, a closed-production pilot will be organized. To which use cases or scenarios this applies will be discovered during the implementation and testing phases of the project, and data protection or other legal and ethical safeguards that may be required will be assessed on a case-by-case basis, taking into account the particular characteristics and risk profile of the pilot.

- OOTS implementation availability

Specifically for BU6 but worth mentioning in this deliverable, the use case assumes that partners involved have an active OOTS implementation available by the time cross border testing and piloting starts. In WE BUILD, no efforts will be supported for implementing OOTS-implementation but just the integration of the wallet with the OOTS.

- Data availability

Use cases essentially work with data coming from (authentic) sources. During designing of the scenarios use cases made a strong effort to ensure the availability of all sources in all (issuing) countries for piloting. Although these efforts have brought a good coverage of the needed data, several use cases did not manage to find a 100% coverage. This means that in some cases, some (authentic) sources will be missing.

To cope with this, the use cases keep on recruiting partners to fill the gaps. Additionally, use cases will make use of QTSP-services to issue the attestations where relevant (authentic) sources are missing. Here, (online) forms will be used to produce attestations to meet the prerequisites for piloting.

- EUDIW availability

For scenarios where an EBW is used and natural persons are using an EUDIW for authentication and authorization (to use the BW), scenarios assume that natural persons are

willing to use an EUDIW. Usage is voluntary by law, but in the context of piloting a necessary prerequisite for execution of the process.

- Mandate related attestations

In the use cases, several mandate related attestations exist. WE BUILD chooses to use 3 types in particular, to validate the mandate (despite other types of attestations may partly include information on this).

- Powers of Attorney

A formal, legally-traceable delegation of authority: an organization grants a specific individual the right to act or make decisions on its behalf for a defined purpose and validity period. It is issued by a Qualified Trust Service Provider based on authentic-source data such as mandate or company registers, and delivered as a signed Electronic Attestation of Attributes (potentially a QEAA) to the person's (Business) Wallet. Explicitly out of scope: informal mandates not registered in an authentic source (e.g. contract-based mandates) or mandates based merely on a company role (e.g. a CFO's purchasing authority).

- Powers of Representation

An attestation proving that a natural or legal person (the "Proxy") holds statutory representation power over the company as a whole — for example, a registered director or legal representative. It is issued by a QTSP acting on behalf of an authentic source (typically a Business Registry) or by a public sector body responsible for that source, and it links the Proxy's identity, the company's identifier (EBWOID), and the scope/limitations of the granted representation power. Because it is tied directly to the authentic source, revocation is automatic if the source updates the person's representation status

- Powers of Employee

A lower-assurance attestation that a person is an employee of a company with a certain role or scope of authority. Unlike PoA and PoR, it is issued by the company itself (as an EAA, not a QEAA) and is not backed by any authentic source or QTSP. Relying parties verify it against the issuing organization's own identity (EBWOID/EUCC) rather than the EU Trusted List, and — critically — the meaning of its role/scope attributes cannot be interpreted generically cross-border; it depends on a semantic model pre-agreed between the issuing organization and the relying party.

6. Expected learnings

The Large Scale Pilot aims to mature the infrastructure for digital wallet usage in Europe by actually implementing it, but also to learn about it and provide recommendations for implementations and improving regulations. In several areas, learnings will be the first of learnings as no previous work had been done on the matter. These learnings will be ‘first learnings’ and perhaps not yet fully curated ‘best practices’.

Work Package 2 applies a domain perspective within these objectives, looking for lessons and recommendations to increase adoption and scalability within the BUSINESS and SUPPLY CHAIN domain. Use cases have their individual learning goals targeting specific areas within the industries, evaluating business value, the use of attestations and related standards, the impact of digital wallet usage and integration on business processes and regulatory challenges. Overall, this leads to the following learning goals in the work package.

6.1 Integration of wallet trust into existing operational sector ecosystems

Learn how digital wallet-based trust in identification and attestations can be integrated with existing transactional and operational systems (e.g. access control, transaction processing, compliance/back-office systems) without major disruption, and what technical and organisational patterns are most effective.

6.2 Use of attestations as reusable trust anchors across processes

Understand how a shared set of attestations (identity, representation, tax, business attributes, etc.) can be reused across multiple processes and contexts—such as onboarding, access control, data sharing and transaction execution—and what constraints or extensions are needed to make this reuse practical.

6.1 Attestation usage across processes

Learn how different types of attestations can be combined and reused across multiple processes and contexts, without creating excessive complexity for issuers, holders and relying parties. This includes understanding which attestation sets are sufficient for typical cross-border situations, how to avoid unnecessary duplication, and how to manage the lifecycle of attestations when they are consumed in different flows over time.

6.3 User Management and Delegation of Rights

Understand how users and organizations can most effectively manage access rights and representation in wallet-based interactions. This covers assigning and revoking mandates, delegating specific rights to employees or third parties, handling different roles for the same person or organization, and ensuring that these mechanisms remain usable and understandable for all actors involved.

6.4 Wallet Dance

Explore how interactions between digital wallets, relying parties and supporting services can be orchestrated across entire process chains, rather than as isolated steps. The goal is to identify robust patterns for sequencing, error handling and fall-back options that work for both

human-centric and automated flows, while keeping the overall interaction as simple as possible for end users.

6.5 Trust infrastructure needs

Several business-domain use cases have strong requirements on identity matching that go beyond the current PID or EBWOID data schema attestation — notably BU2 (opening a foreign branch abroad) and BU3 (tax declaration and request of a tax ID attestation). Business registries and tax authorities acting as relying parties have high identity-verification standards and specific attestation requirements. Public services in BU6 (access to OOTS) and BU3 require a service-based power of attestation authorization as a prerequisite. This implies establishing the right relying-party registry with a catalogue of attestation types to ensure digital wallet interoperability.

The trade-off WeBuild made for the pilot — working with a static trusted list with no scalability built-in and no live trust infrastructure — is a learning by itself : we chose the simplest available trust anchor (verifier-knows-issuer / static list) from the available options (EU Trust List per ETSI TS 119 612, EBSI, OpenID Federation, verifier-knows-issuer), because a queryable RP registry with an attestation-type catalogue and live trust infrastructure does not yet exist at scale. The gap is governance and infrastructure, not protocol. DCQL trusted authorities is the mechanism that would allow business registries, tax authorities and other relying parties to constrain accepted issuers once those registries exist. In practical terms, this means not just "give me a credential of type X" but "give me a credential of type X issued by an authority I trust."

The learning coming from our piloting is the ecosystem need for a production-grade EU registry of authorized EBWOID issuers, or business registry attestation issuers, or PoA issuers (and other mandate attestation issuers), that a digital wallet can query against a standardized API. The protocol mechanism exists. The infrastructure it points to is not built yet.

Finally, the pilots shall help us to understand what it really takes to keep authorizations and credentials trustworthy over time in dynamic, cross-border business relationships. The project wants to learn how revocation, status changes and trust-anchor failures play out in realistic scenarios (e.g. intermediary changes, company restructuring, mandate withdrawal) and whether the current trust models in ARF (and future implementing acts) are sufficient. It also seeks clarity on what governance arrangements and monitoring mechanisms are necessary so that Member States and market actors can rely on digital wallet-based attestations at scale without creating unmanageable operational risk.

6.6 User Experience

Assess how digital wallet-based interactions are perceived and handled by users in realistic settings, and what design choices improve or hinder adoption. The focus is on clarity of consent and data disclosure, effort required to complete tasks, error recovery, and the impact of different device, channel and interaction choices on overall satisfaction and trust.

6.7 Attestation Standardization

Understand to what extent attestation models can be standardized and reused across countries, sectors and use cases, and where variability is unavoidable or even desirable. This includes testing how well common models cover diverse legal and operational requirements,

identifying areas where additional attributes or constraints are needed, and deriving recommendations for future standardization work.

6.8 Machine-to-machine

Learn how wallet-based attestations can be issued, presented and verified in unattended, system-to-system exchanges (e.g in the supply chain domain) without requiring a human holder or per-transaction interaction and what technical and organisational patterns (e.g. policy-driven presentation, backend integration into transaction-processing systems) are most effective.

6.9 Identifier and discovery reuse

Learn how wallet-based organisational identity and discovery can be integrated with existing business identifier schemes and directory/discovery infrastructure.

7. Challenges and risks

7.1 Introduction

This chapter addresses the main challenges and risk existing for the use cases and scenarios in work package 2. This will include any challenge or risk that also applies to work package 2 or in general, to provide a complete overview.

All will be monitored and – if possible – reduced/mitigated during the next phases of the project (implementation, testing and piloting) to maximize the output and value from work package 2.

7.2 Main challenges

The main challenges which the use cases in the work package are currently facing are the following

- Partner involvement

Chapter 2 mentioned that per use case, or even per scenario, a core team of people and partners emerged during the stock-taking and specification phase. This core team was producing most of the work, attending most of the workshops and meetings and showed the strongest commitment.

This pattern is not uncommon in the beginning of LSPs: a core team producing and a surrounding group reviewing and following. In the work package, the policy had clearly focused on making the results of a use case/scenario, a group result. Meaning all partners must commit or at least consent to the decisions that were made.

Moving on to the implementation, testing and piloting, it is clear that the core group is no longer sufficient to make the pilot a success. All partners must implement, test and pilot to give the use case the body and significance it needs to learn and present its results. At the end of the specification phase, all partners were therefore explicitly asked to reconfirm their commitment for piloting. And during implementation, very close monitoring of progress will be applied, using several smaller milestones like connecting to the Interoperability Test Bed and using test reports. Differences in (implementation) velocity is expected across partners but sets of ‘earliest-dates’ and ‘latest-dates’ will be set, to give all partners some freedom to manoeuvre but also be very clear on what is expected in terms of progress.

- Evolving environment

During the stock-taking and specification phase, several fundamental frameworks were identified. Of course the framework for the EBW is developing in parallel of WE BUILD unfolding itself. This is perhaps one of the most fundamental elements for the entire project, being strongly connected to the purpose of the project.

With completing the specification phase, the use cases have produced the specifications, scope decisions and working assumptions for all scenarios. A level of maturity and agreement has been reached, that will be the stable foundation for all technical development of the use case software and infrastructure.

To secure the stability and control, WE BUILD will apply strong change management throughout the remainder of the project. This means that for every change in the environment of the project, like in the ARF, the EBW frameworks and other regulations, WE BUILD will assess the impact of the changes and will decide about adopting all or part of the changes in the project. This way, the project prevents introducing moving targets in the project, or at least uncontrolled moving targets. Change is expected, but in a controlled way without jeopardising the project results.

- Incompleteness in frameworks, standards and regulations

In line with the previous point, the use cases have been challenged during the specification phase, by several gaps and ambiguous elements in relevant frameworks, standards and regulations. To cope with this, the use cases have established several working assumptions. The gaps and ambiguities are expected to continue offering challenges during implementation and testing of the use cases and scenarios.

At best, working assumptions will be confirmed by future versions of regulations, standards and frameworks. To increase possibility, narrow collaboration with standardization bodies is performed as much as possible. Worst case, future versions of regulations and frameworks chose conflicting directions, or gaps / ambiguities remain.

For best control in WE BUILD, the use cases maintain an overview of working assumptions in order to cope with gaps and ambiguities, as well as apply strong change management on changes in frameworks and regulations.

In any case, the use cases will choose clarity and continue (instead of waiting for clarity) and will learn from piloting.

7.3 *Main risks*

Next to the challenges that the use cases already experience, mentioned in the previous section, the work package has identified the following main risk that may affect the project activities during the remainder of the project.

- Time versus ambition

Discussions during the specification phase, to find the proper balance between value and feasibility have been extensive. It is clear that strong opinions on directions, scope, solutions and priorities exist.

The scenario specification documents that have been produced during the specification phase should provide clear guidance during the remainder of the project.

However, previous LSPs show that during implementation new, unknown challenges will unfold. These may introduce extra pressure on the development of the infrastructural and software solutions, requiring revisiting some of the discussions on priorities and scoping of scenarios and use cases. Especially, because of the time constraints that exist in the project: the project must be completed by September 2027.

Discussions from during the specification phase show that discussions on the balance between value and feasibility are intense and can be time-consuming and disorienting.

To cope with this, the domain leads and work package leads will be stronger involved in these processes, forcing discussions to be completed quick and adequate, maintaining the focus in the project as well as safeguarding delivery of results targeting the core of each use case.

- Velocity during development and testing

During implementation, significant differences in velocity of development and testing are expected across all partners involved in the use case scenarios. Although this is expected as this is a regular phenomenon during LSPs, it will prove difficult to cope with once it occurs. Differences in implementation velocity often result from differences in starting points (some partners already have a digital wallet-related infrastructure available while others don't), differences in resource availability and/or differences in priority (competition with other local projects that exist in the partner-organization).

The different velocities will result in some partners being ready for (cross border) testing earlier than others. A minimal set of partners is needed to establish a working cross border ecosystem, to perform tests and pilots at all. Differences in velocity offer challenges because it could take long before that minimum set of partners is available. Also it could offer challenges for partners that are ready earliest, as they need to wait a longer time in order to test with partners that require more time to complete their implementation.

The differences in velocity may turn out difficult to manage. In the end, the project has a clear closing date that needs to be met. Differences in velocity form a threat for meeting the KPIs of the project, but also for collecting sufficient learnings from piloting.

The risk will be monitored closely by use case leads. On a work package and project level, interventions could be implemented where partner implementations for certain use cases will be prioritized over other use cases, to ensure the over-all success of use cases in the project as a whole.

- Dependencies between use cases

Many dependencies exist between use cases, especially in terms of attribute issuance. Several types of attestations are used by more than one use case. Use cases count on other use cases to take care of issuance of these attestations, for certain countries. For example BU3 counts on BU4 to issue a PoA attestation for Finland, so BU3 can use that in their pilot. These types of dependencies have been carefully monitored. Requirements from use cases were processed by other use cases when designing attestations.

During implementation though, it may turn out that requirements weren't fully correct, or correctly processed into the design due to differences in interpretation. Even changes in requirements or (small) scope changes, can result in other use cases not (completely) pilot their processes. Also one delay (or drop) of issuance of such an attestation for one country can immediately impact several other scenarios of other use cases.

The number of dependencies across all scenarios and countries is considerable and will be carefully monitored during implementation and testing. A small reduction in pilotable country-combinations is to be expected but should not affect the KPIs and learnings.

8. Conclusion

This deliverable has established the pilot design for Work Package 2 of WE BUILD, covering digital wallet-enabled use cases in both the Business and Supply Chain domains. It consolidates the results of the stock-taking and specification phases into a coherent set of scenarios, attestation designs and working assumptions that are ready to guide implementation, testing and piloting.

The pilots span 27 high-priority scenarios, complemented by a set of stretch-goal scenarios that can be implemented where capacity and feasibility allow. Together they address a broad range of cross-border situations, from business onboarding and representation to operational interactions, data sharing and transaction execution, while reusing a common set of attestation and trust components as much as possible.

Throughout the work, strong emphasis has been placed on managing dependencies between use cases and aligning across domains. Shared attestations, common mandate and representation models, and reusable digital wallet and trust infrastructure have been designed through structured cross-use-case collaboration and close coordination with other work packages, notably those responsible for architecture, technology, business models and communication.

The expected learnings set out in this document provide a clear agenda for the upcoming piloting phase. They focus on attestation usage across processes, user management and delegation, the choreography of digital wallet interactions, trust infrastructure and governance, user experience in real-world contexts, and the standardisation and reuse of attestation models. Insights from piloting are strongly related to the 6 key-objectives of the project and will feed into subsequent work package deliverables and into broader discussions on future large-scale deployment.

At the same time, the challenges and risks identified for the pilots remain significant, including evolving standards and regulation, multi-country and multi-partner coordination, and the need to deliver meaningful results within the available time. Work Package 2 will continue to manage these through prioritisation of scope, active engagement of partners, structured change management and close monitoring of feasibility and progress.

This deliverable should therefore be seen as the current baseline for the Business and Supply Chain pilots in WE BUILD. It defines the intended scope, priorities and learning focus for Work Package 2 at this stage of the project, while recognising that limited adjustments may still occur during implementation, testing and piloting. Those adjustments will be reflected in the final Work Package 2 deliverable.

Annex A – Use case / attestation matrix MVP/MVP+

	BU1	BU2	BU3	BU4	BU5	BU6	SC1	SC2	SC5
A1									
Approved supplier attestation									
Authorized service provider attestation									
Business license									
Certificate of tax residence									
CompanyInfo									
ContactPerson									
ControlList									
DUNS									
EBWID									
eCMR									
Electronic invoice									
Employee VC									
EU PoA									
EUCC									
ESG									
IBAN (= confirmation)									
IBAN OV									
Legal Entity Identifier									
Membership credential									
Microcredential									
OwnershipList									
PaymentTerms									
PID									
PoA									
PoE									
PoR									
PWN									
QES (not country bound)									
Service based authorisation									
SiteAttestation									
Social security attestation									
Tax Nr									
UBO									
VAT ID									
Verifiable skill									

Annex B – Use case / country matrix

BU1		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	AT										
	CH										
	DE										
	ES										
	FI										
	FR										
	IT										
	NL										
	NO										
	PL										
	PT										
	SE										
BU2		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	ES										
	FI										
	FR										
	NL										
	NO										
	SE										
BU3		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	ES										
	FI										
	NL										
BU4		Scenario 1a		Scenario 1b		Scenario 1c		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	AT										
	BE										
	DE										
	ES										
	FR										
	GR										
	IT										
BU5		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	GR										

	SE										
BU6		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	GR										
	NL										
	PL										
	PT										
	SI										

SC1		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	BE										
	DE										
	ES										
	EE										
	FR										
	NL										
	PL										
SC2		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	BE										
	FI										
	SI										
SC5		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	BE										
	DE										
	ES										
	FR										
	GR										
	NL										

Annex C – MVP scenario specification documents

Use Case	Scenario ID	Name
BU1	1	KYC (B2B vertical)
	2	KYS (B2B vertical)
	3	KYC (soletrader)
	4	KYS (soletrader)
	5	KYE
BU2	1	Create a Company Branch in an EU or EEA Member State
	2	Register Branch for Tax
BU3	1	Filing VAT-declaration using Tax Portal
	2	Filing VAT-declaration using M2M Interaction
	3	Issuing VAT certificate using Tax Portal
	4	Issuing VAT certificate using M2M Interaction
BU4	1a	Issuance PoA attestations
	1b	Issuance PoR attestations
	1c	Get access to service
BU5	1	Micro-credentials
BU6	1	Full power authentication at OOTS online procedure portal of evidence requester and at OOTS evidence provider side e.g. preview space of evidence provider
	2	Fine-grained power authentication at OOTS online procedure portal of evidence requester and at OOTS preview space of evidence provider
SC1	SC1.1	Enrolment and trusted contracting
	SC1.2	Identify and security access
	SC1.3	Cross border transport. Digitalize logistics eCMR
SC2	1	Onboarding CEADS
SC5	1	Supplier pre-approval
	2	Service Provider authorization
	3	Service Provider authorization verifiable by Tax administration
	4	Direct eInvoicing using Business Wallet

WE BUILD consortium

Specification Scenario 1 – KYC (B2B vertical)

WP2 – BU1

Date : 19.06.2026
Version : 1.0
Status : final

Table of Contents

1 Introduction.....	3
1.1 Objectives of this document	3
1.1.1 Requirements Status by Project Phase	3
1.1.2 Major assumptions	3
1.1.3 Important Architecture Design Records (ADRs)	3
1.1.4 Most important open topics	3
1.1.5 Most relevant points for future revisions	4
1.2 Scenario introduction.....	4
2 Scenario specification.....	6
2.1 Introduction	6
2.2 Scenario pre-conditions	6
2.2.1 MVP Restrictions	7
2.2.2 Planned MVP+ Extension	8
2.3 Issuing the required attestations.....	8
2.4 Scenario main flow.....	9
2.4.1 Legal Entity Selection.....	13
2.4.2 Use Case specific additional Data (MVP+).....	13
2.4.3 Legal Entity Identification	14
2.4.4 Organisation Structure.....	15
2.4.5 Additional Identifiers (LEI) (MVP+)	16
2.4.6 Fraud & Sanction (MVP+)	17
2.4.7 Use case specific cross check & transfer in the internal system.....	18
2.5 Scenario additional flows	18
2.6 Challenges and barriers	19
2.7 Working Assumptions	20
3 Detailed scenario flow	21
4 Roles and participants.....	24
4.1 Scenario roles and participants.....	24
4.2 Additional roles and partners	24
4.3 Target country combinations.....	25
4.4 Requirements.....	25
5 Attestations	26
5.1 Introduction	26
5.2 Attestations to be provided by other UCs/WGs/scenarios.....	26
5.3 Created attestations in the scenario	27

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 1, as part of use case BU1 in Work Package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.1.1 Requirements Status by Project Phase

MVP Requirements Status	MVP+ Requirements Status	General Comments
1.0	0.7	MVP: final version MVP+: ongoing

1.1.2 Major assumptions

The assumptions outlined here are affecting the Use Case as a whole and may include assumptions with regard to chapters 4 () and 5 (). Detailed assumptions regarding the inner workings of the itself (chapter 2) can be found in chapter 2.7 ().

Assumption	Related discussions (excerpt)

1.1.3 Important Architecture Design Records (ADRs)

ADR	Short description

1.1.4 Most important open topics

Topic	Description	Responsible	Resolved

1.1.5 Most relevant points for future revisions

Topic	Description
Chapter 2.3 ()	The chapter was introduced on request of workstream leads_after_peer review to give a short introduction regarding different sources of attestations to the reader. This chapter serves as a business hinge to our and other workstreams deeper work and by nature does not replace more specific documentation.

1.2 Scenario introduction

The BU1 scenario 1 use case aims to redefine a core flow for European businesses. The objective of this use case is to demonstrate the applicability of the EU Business Wallet for companies in the process of Know Your Business Partner due diligence with regard to fulfilling regulatory obligations as well as business obligations in general. Digitising Know Your Business Partner processes improves trust, transparency, and compliance while significantly reducing onboarding time and cost—especially in cross-border contexts.

In this scenario the context is Know your Customer (KYC).

- Company A (country A) wants to enter into a business relationship with another company B (country B) and wants to become a customer of company B.
- Any employee of company A is initiating the process of issuance and presentation of required KYC attestations.
- Authorisation is out of scope of this scenario.

A process based on verifiable, interoperable, and reusable organizational attestations has the following benefits for the market:

- a. Faster establishment of cross-border business relationships
- b. Reduced fraud and compliance risks
- c. Increased efficiency and competitiveness for European enterprises
- d. A resilient and trustworthy digital single market

The scenario is based on the following documentation:

1. **BU1 Stock Taking document:**

<https://portal.webuildconsortium.eu/group/bu1->

kyskybddd/files?mid=5921&fid%5B0%5D=11&fid%5B1%5D=12&fid%5B2%5D=4188

2. **WE BUILD Architecture & Integration Blueprint:**

<https://portal.webuildconsortium.eu/topic/d41-architecture-integration-blueprint-reference-document>

3. **EBWOID Data schemas & Issuance rulebooks:**

<https://portal.webuildconsortium.eu/topic/ms14-pid-ebwoid-data-schema-issuance-rulebook>

2 Scenario specification

2.1 Introduction

This scenario pilots the onboarding process for enterprise customers (named as Buyer in diagrams) seeking to procure goods and/or services from enterprise suppliers (named as Seller in diagrams). To satisfy standard due diligence requirements, the goods and/or service provider mandates that the customer present a specific set of digital attestations to verify their corporate identity.

As MVP within the BU1 (KYS/KYC/KYB/DD) use case, this scenario is conducted using a European Business Wallet (EBW).

1. Natural persons act on behalf of their organisation; neither their personal identity proofing nor their authorisation is not part of this scenario.
2. No attestations are issued to or presented from an EUDI Wallet. The case of a sole-trader using the EUDI Wallet will be pilot in the scenario 3 and the process from Relying Parties should be aligned here.

2.2 Scenario pre-conditions

To ensure the successful execution of this scenario, the following entities and technical frameworks must be active and accessible:

1. **Established EBWOID Issuer and EU Business Wallet Provider:** The legal entity must have access to a European Business Wallet (EBW) as defined in the Architecture & Integration blueprint. This wallet must be issued by a recognised provider, active and initialised with the required Business Wallet Owner Identification Data (EBWOID) to uniquely identify the business in a digital context.
2. **Availability of Specific Digital Attestations:** The two business parties must have successfully requested and stored the following credentials within their wallets:
 - EBWOID
 - EUCC
 - Tax number (Open Point – to be discussed - see options)
 - VAT

- ContactPerson
- OwnershipList
- ControlList
- CompanyInfo
- WUA (MVP+)

For solving the Tax issuance we have 4 options:

Description	Status
specified by the company (as input value) - similar paper document today	Accepted by the Relying Party (Bank) now, but not suitable for future product selection.
Company issues its own Electronic Attestation of Attributes (EAA)	Similar issues to the paper-based method.
Tax Administration issues the attestation (as an EAA)	A desirable future solution with guaranteed acceptance from the Verifier.
Company Register issues it as a Public EAA (Pub-EAA).	An alternative solution that also has acceptance from the Verifier.

- 1. Harmonised Trust Framework for EAA Verification:** A functional Electronic Attestation of Attributes (EAA) verification layer must be operational. This relies on a harmonised trust framework that allows the Verifier to instantly cryptographically validate the authenticity and integrity of the data provided by the Business Wallet.
- 2. Mutual identification & selection of the business wallet:** This is required in order to initiate the KYC flow and shall follow the WE BUILD-Blueprint as well as available technological options within BU1 Scenario 1.

2.2.1 MVP Restrictions

- **Reduced Verification & Trust Reliance:** Neither seller nor buyer wallets perform full verification of attestation issuers or wallet integrity. If EAA providers are included in the WE BUILD specific trust lists (trust infrastructure) and the Wallet Provider support the WE BUILD trust lists, then EAA issuer verification can be demonstrated. However this solution cannot be used after WE BUILD ends. The member states have explained that only QTSPs can be included in the TLOL (trusted list of lists) also due to scalability reasons. Therefore, the WE BUILD-specific TLOL is not applicable outside of the

consortium, and therefore only a showcase.

Implication: The system relies on assumed trust rather than cryptographic validation, posing risks in high-assurance scenarios.

- **Limited Mutual Identification:** Seller and buyer wallets lack robust features for securely identifying each other. The seller wallet does not provide the attestations that allow the buyer wallet to identify the seller. The verifierInfo object including the EBWOID and WUA of the seller wallet is not provided when the presentation request is created. The corresponding verifierInfo object is not defined yet.

Implication: Advanced peer-to-peer identification and consent workflows using attested identities and wallet unit attestations are not yet supported.

- **Process & Risk Simplifications:** The MVP assumes all suppliers are low/medium risk, executes processes sequentially, and lacks cross-attestation checks or internal system integration.

Implication: Limits handling of complex risk scenarios and data consistency.

- **Confidential Data Restrictions:** Current EBW versions cannot securely present highly confidential attestations due to missing security configurations.

Implication: Restricts use cases to synthetic sensitive data.

2.2.2 Planned MVP+ Extension

- If the EBW wallet and trust infrastructure limitations documented in the chapter 2.6 () are removed then the above mentioned limitations will not apply to the MVP+.
- The process will be still executed in one step (more steps are not required).
- Additionally support for Additional Identifiers, UBO, Fraud&Sanction, ESG (MVP+)

2.3 Issuing the required attestations

Before the KYC process can be executed, the Buyer's EBW must be provisioned with the required attestations. These attestations are categorized into two primary types:

1. **Externally Issued Attestations:** the majority of these attestations represent assertions made by authoritative external entities. These may include public sector bodies (such as official business registers) or private entities (such as conformity assessment bodies). Users can request these attestations either

through the respective issuer's external portal or directly via the EBW, which may feature a pre-configured set of attestation requests for supported issuers.

2. Self-Issued Attestations: Certain information cannot be validated by external entities and must be asserted directly by the attestation subject. These attestations are generated using a local issuer component, which is ideally integrated natively within the economic operator's EBW.

The issuance process for this use case strictly follows the [workflow defined by WP4](#).

A current overview with regard to the issued attestations during BU1 KYC MVP can be found in . *The exact process of issuing attestations, however, belongs to the rulebooks and is not part of this document.*

2.4 Scenario main flow

The onboarding journey begins when a person navigates to the Seller's website and selects the desired product or service. To facilitate clear communication

- **Block1:** the initiator selects the appropriate method for the data exchange between their own EBW wallet and the respective business partner. This can be done via URI, a direct integration to the Wallet or endpoint retrieval.
- **Block2:** the initiator provides the companies contact details, ensuring that all subsequent status updates and results reach the correct stakeholder.

In order to be flexible, the process is built using building blocks Block1 and Block2 which can be adapted for each company requirements. In the MVP we will demonstrate the order specified above (B1 then B2).

With the endpoint identified, a critical security handshake occurs: the Seller's and the Buyer's Business Wallet perform mutual identification. This ensures a trusted connection before any sensitive data moves. Upon successful verification, the wallet shares the base business data.

The process then moves into a dynamic phase where the Seller requests additional application-specific attestations. Depending on the complexity of the service, this exchange may iterate multiple times to satisfy all compliance requirements. Finally, once all requested attestations are successfully validated, the data is integrated into internal systems for processing, and the applicant is promptly notified of the result.

The following figure depicts an overview of the process:

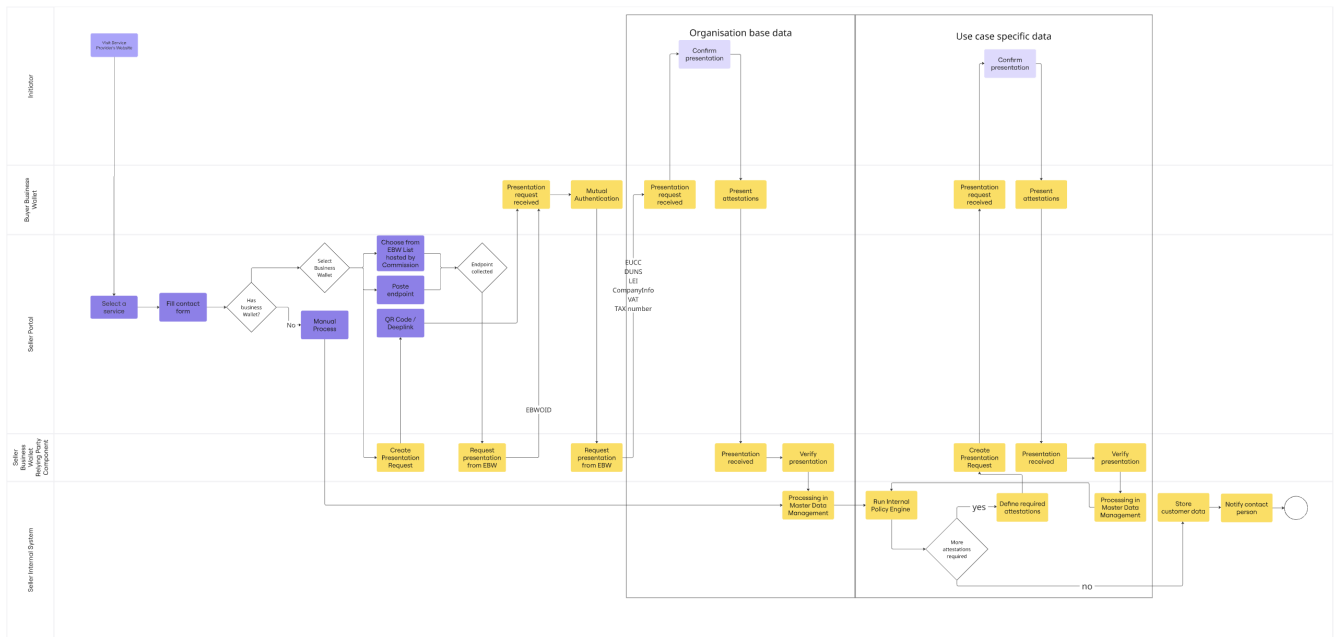


Figure 1: [Process Overview](#)

The required actors and software systems for the flow detailed in the following interaction diagrams are:

- Software systems owned by the buyer legal entity
 - Buyer Business Wallet: EBW wallet of the buyer that acts as a customer EBW primarily in the holder role during this workflow
- Software systems owned by the seller legal entity
 - Seller Business Wallet Relying Party Component or Seller Business Wallet: EBW wallet or Wallet Relying Party Component of the seller that acts in the EBW Relying Party.
 - Seller Portal: Web application owned by the seller legal entity that acts as a frontend for customer employees.
 - Seller Internal System: ICT systems owned by the seller, into which the presented data is transferred, e.g. enterprise relationship management system or customer master data management system.
- Software systems owned by the (Q)EAA providers
 - (Q)EAA provider revocation service: Revocation service for the (Q)EAA provider with unified revocation interface toward the EBW also for QEAA
- Software systems owned by the EBWOID provider

- EBWOID revocation service: Revocation service for the EBWOID
- Software systems for which the national Supervisory Body is responsible
 - Trust List that are part of the TLOL and included the EBWOID provider certificates
- Software systems for which the Wallet Provider is responsible
 - Wallet Unit Attestation (WUA) revocation service: Revocation service for the WUA
- Software systems for which the EAA Provider is responsible
 - EAA revocation service: Revocation service for the EAAs including the self issued EAAs

The following diagram provides an overview of the end-to-end process for MVP and MVP+.

Note: the block specific for the MVP+ are marked with green background in the diagram

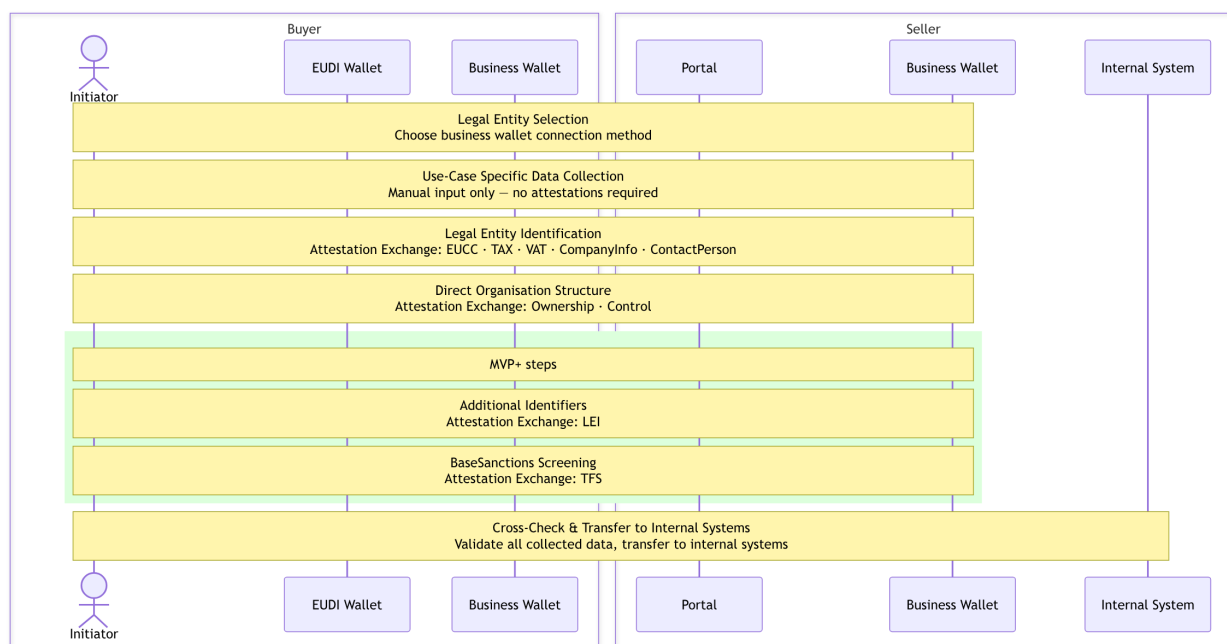


Figure 2: [Workflow Overview](#)

The MVP and MVP+ prerequisites for the scenario are shown in the following interaction diagram.

Note: The block specific for MVP+ is marked in the diagram

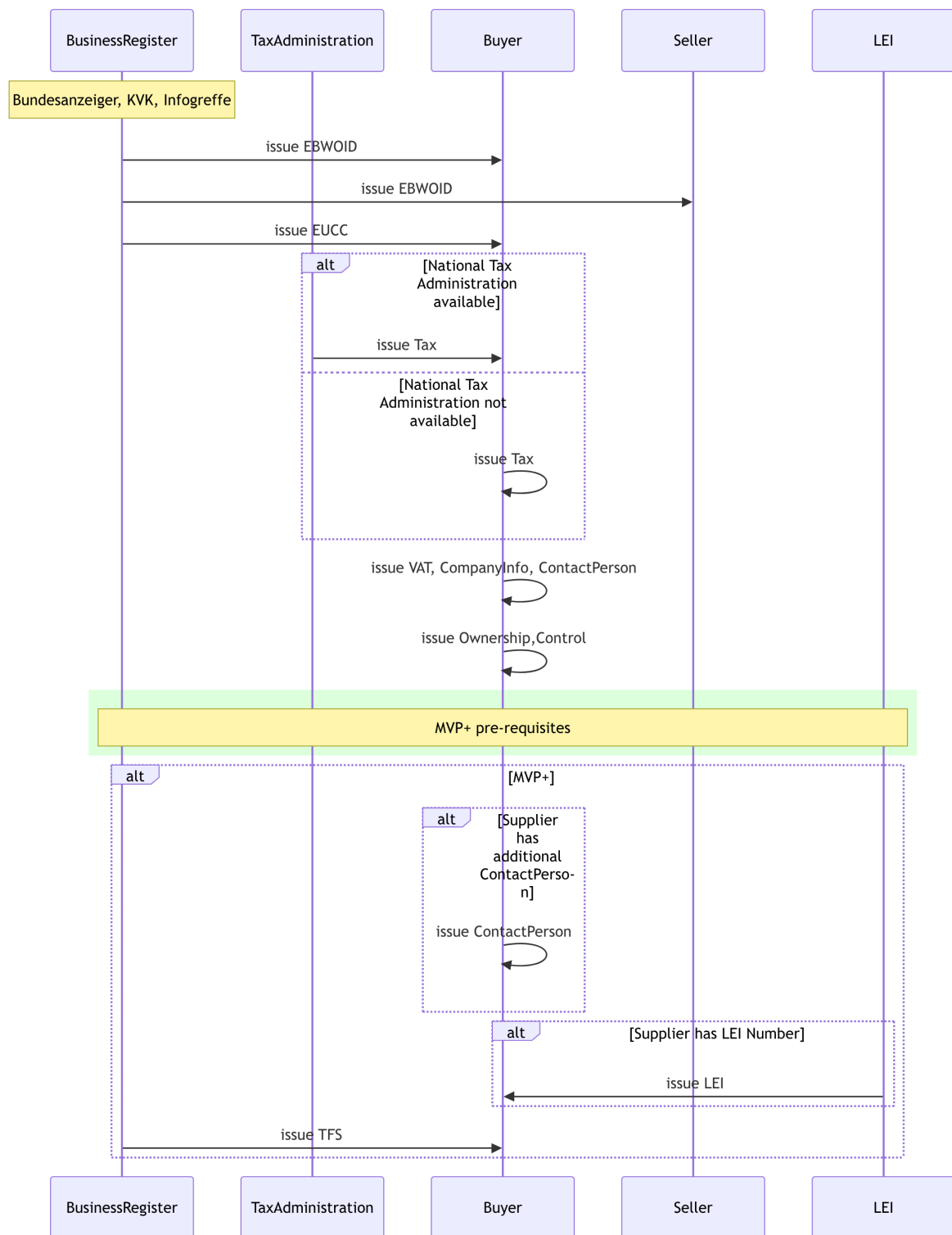


Figure 3: [Prerequisites](#)

The buyers wallet needs all the attestations requested by the seller in his wallet.

The seller needs to provide all the attestations needed by the buyer during mutual identification.

In the following sections, the building blocks of the process are defined in detail.

The process begins when an initiator selects a specific service on the Seller website.

2.4.1 Legal Entity Selection

To ensure seamless communication, the initiator selects the Business Wallet:

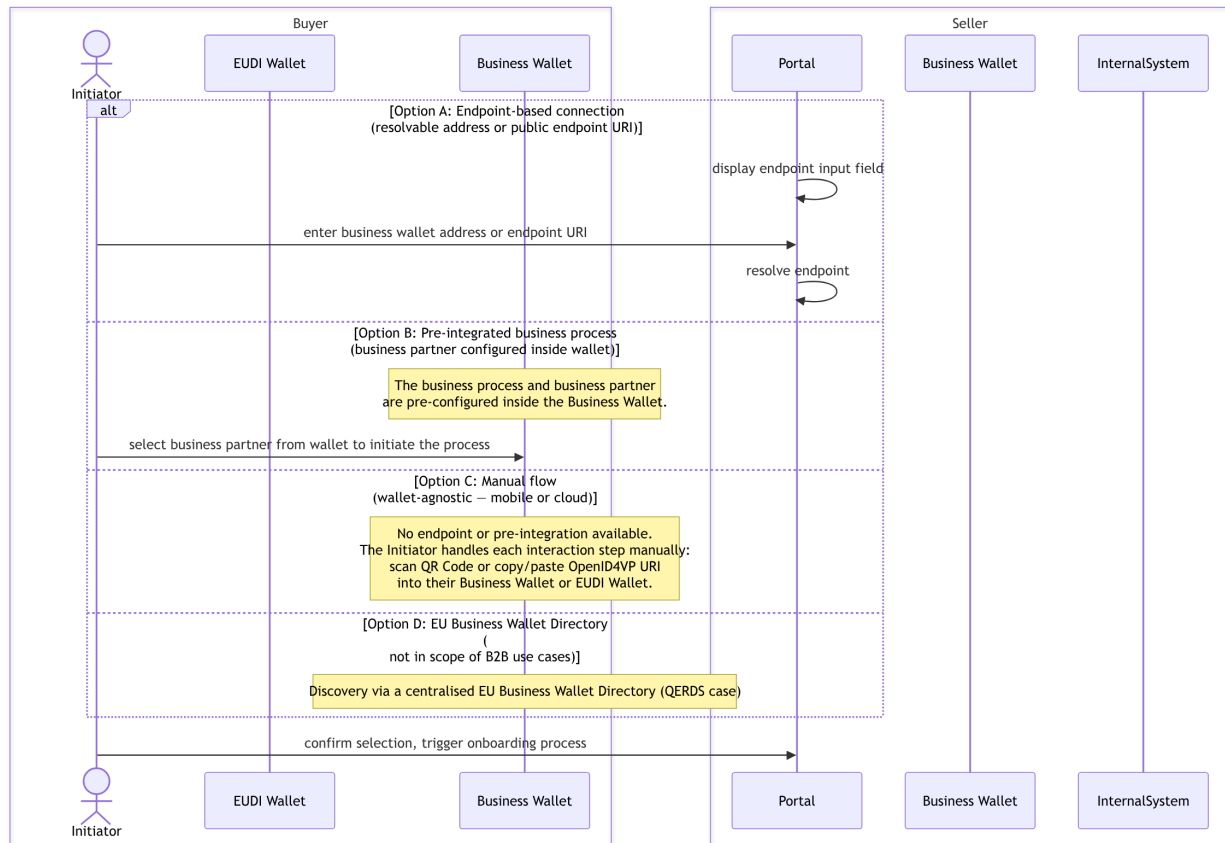


Figure 4: [Legal Entity Selection](#)

2.4.2 Use Case specific additional Data (MVP+)

The following additional info needs to be manually inserted per request for a complete KYC flow (as input):

- Person contact data : name, surname, email address
- Optional telephone

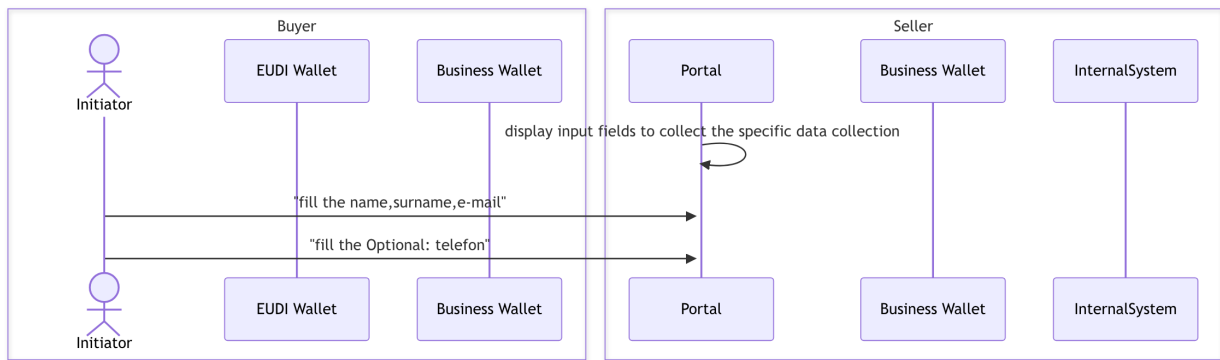


Figure 5: Use Case specific additional data

2.4.3 Legal Entity Identification

The following interaction diagram describes the interaction between the seller and the buyer's company starting with the Portal request to generate a proof request for several attestations which should be presented by the buyers wallet. The step ends after the verification of the presented attestations according to the attestation rulebooks.

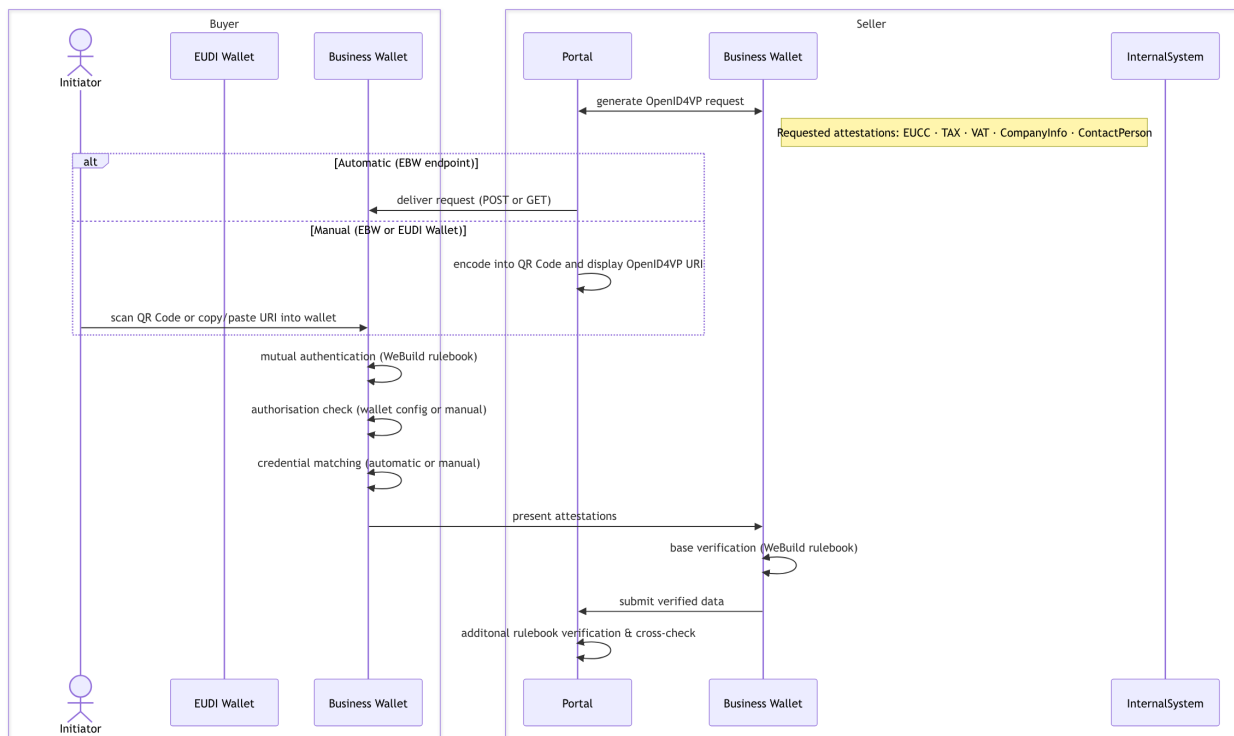


Figure 6: Legal Entity Identification

Before any sensitive data is exchanged, a secure handshake occurs. The Seller Business Wallet and the Buyers Business Wallet perform mutual identification to verify the identity and integrity of both parties.

The mutual identification step is defined and detailed in the following rulebook, that will be reviewed by the architecture group: [[holder-authorization-handshake.md](#)]

After successful identification of the requesting seller wallet, the requested company base data is presented by the buyer wallet:

- EBWOID (required for buyer wallet identification)
- EUCC
- Tax number
- VAT
- Company Info
- ContactPerson

The Wallet Unit Attestation may also be requested by the seller. According to EU Business Wallet regulation Article 14/2/b "...Wallet units shall enable authentication and validation of the Wallet unit components by presenting the Wallet unit attestations...". The WUA revocation status can be used by the seller to avoid requesting data from revoked EBWs (e.g. due to compromise).

For each presented attestation the basic verification steps are performed by the seller wallet.

The basic verification steps are described in the following rulebook: [[verifier-base-verification.md#42-relying-party-obligations](#)].

2.4.4 Organisation Structure

After verification of the base data attestation and running the internal policy engine, it may be necessary, depending on the use case, that additional information is retrieved, in order to finalise the onboarding and set up a contractual relationship.

- OwnershipList
- ControlList

Internal Policy means the company decides on its internal rules who is allowed to receive the attestations based on the business partner selection process. This is required because the information stored here contain very high sensitive data, e.g.: like the private address of an UBO (normally should be always 4 -eyes principle).

The interaction diagram and the performed steps are similar to the steps described in section 2.4.3 ():

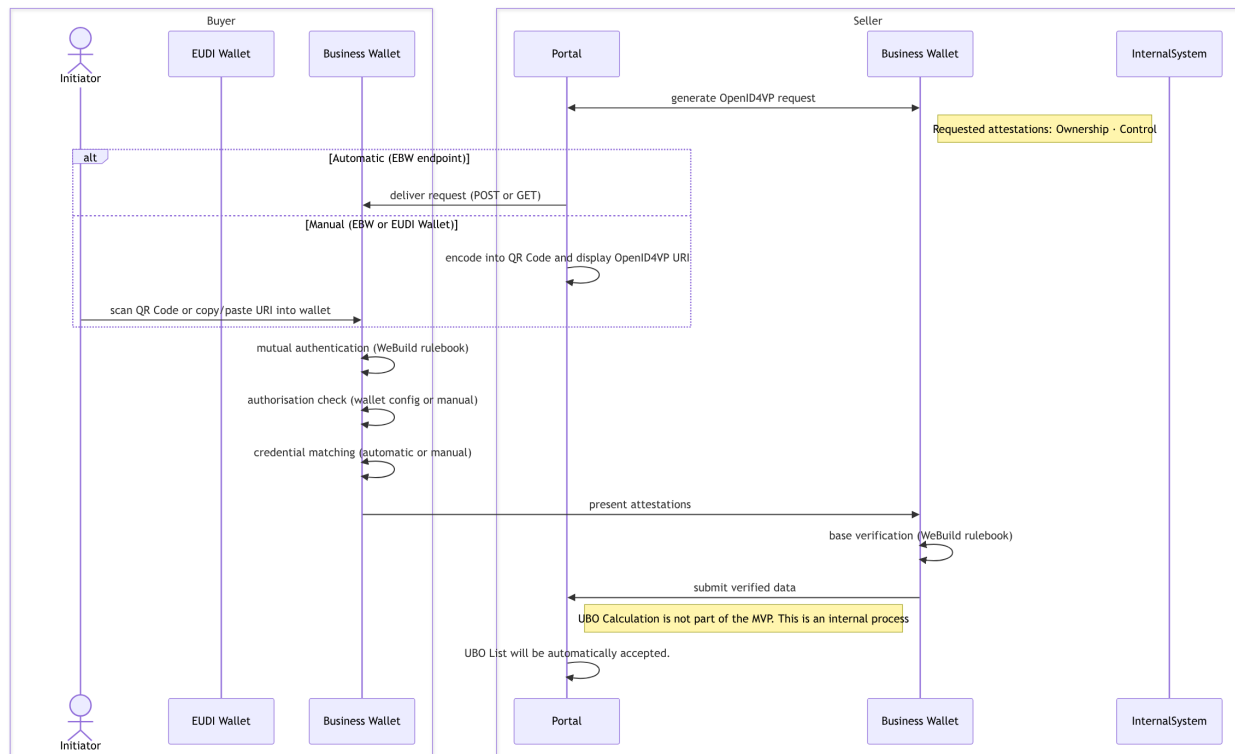


Figure 7: [Organisation Structure](#)

2.4.5 Additional Identifiers (LEI) (MVP+)

After verification of the base data attestation and running the internal policy engine, it may be necessary, depending on the use case, that additional information is retrieved, in order to finalise the onboarding and set up a contractual relationship.

- LEI

The interaction diagram and the performed steps are similar to the steps described in section 2.4.3 ():

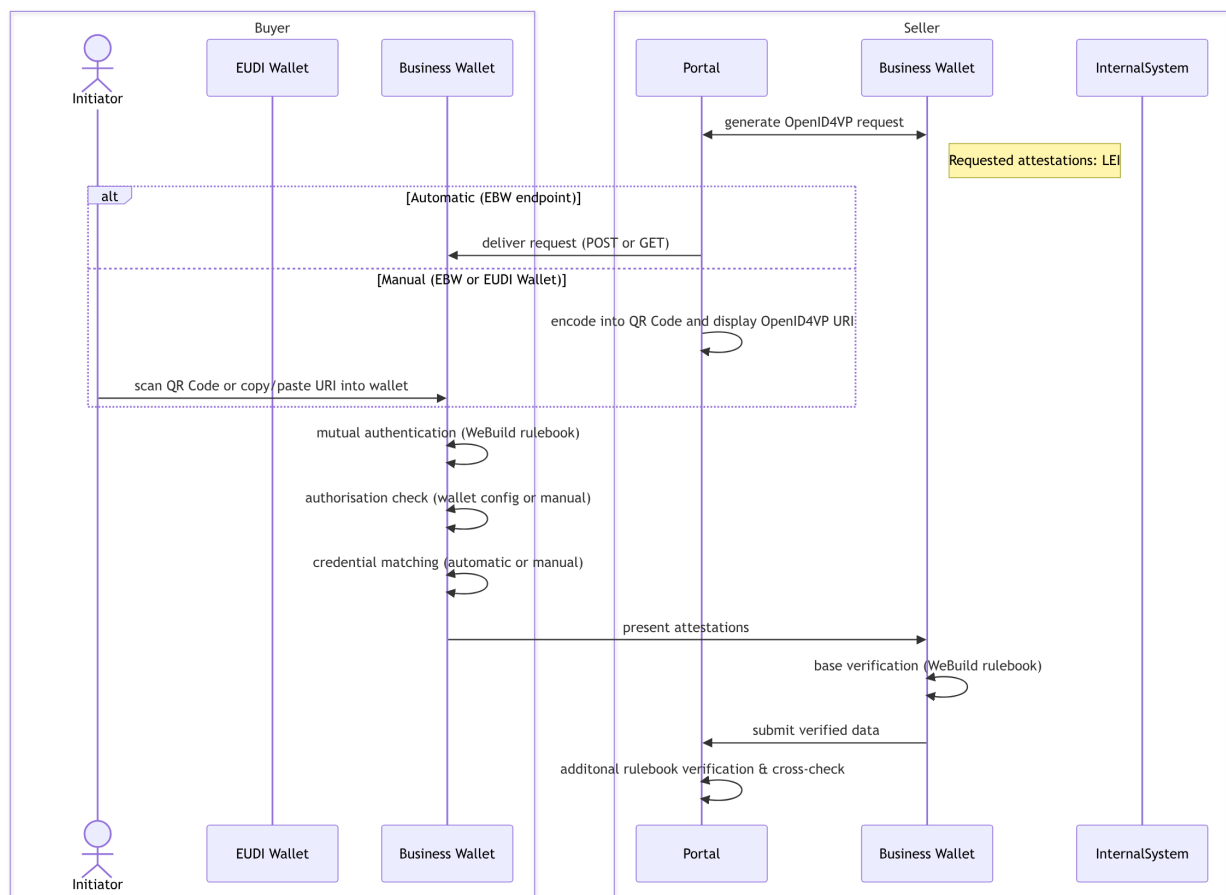


Figure 8: [Additional Identifiers](#)

2.4.6 Fraud & Sanction (MVP+)

Based on the submitted data, the relying party may perform a risk assessment. Depending on the result, additional attestations such as sanction lists may be requested.

The interaction diagram and the performed steps are similar to the steps described in section 2.4.3 ():

Figure 9: [Base Sanctions Screening](#)

2.4.7 Use case specific cross check & transfer in the internal system

After successful validation, the data is transferred to the internal IT systems of the relying party for further processing and the contact person is notified.

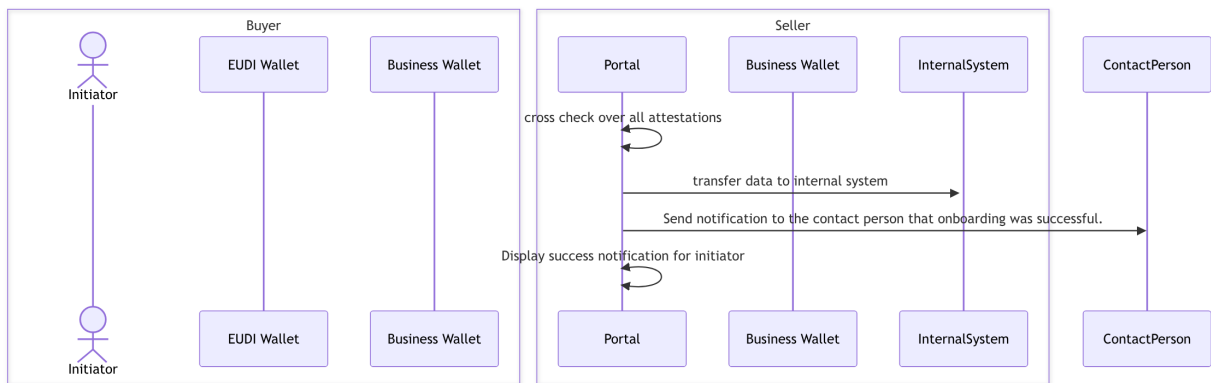


Figure 10: [Cross Check](#)

2.5 Scenario additional flows

Flow Variations	Short description
Tax information available from authentic source	If an authentic source is available for the the country of the customer, tax related attestations shall be issued by these.

Flow Variations	Short description
Tax information not available from authentic source	If no authentic source is available for the the country of the customer, the related attestations shall be issued as a self-issued attestation.
LEI for financial applications	If the context is in the financial sector, an LEI attestation shall be requested by the service provider.
User consent	In this variation, the Business Wallet user gives consent to present data with the relying party.
Automated consent	In this variation, the Business Wallet is configured to give consent based on a policy engine.

2.6 Challenges and barriers

The scenario depends on multiple architecture decisions such as the implementation of mutual identification, consent management in the business wallet, EAA verification, and attestation chaining. Due to the complexity and number of attestations required within the scenario, semantic alignment is paramount to achieve interoperability between participants and between use cases sharing attestations. Therefore, a mechanism for appropriately defining semantics is required.

The above restrictions described in “MVP and MVP + Restrictions” are due to:

- Missing agreement to the ADR EAA provider identity verification based on chaining and TLOL that is needed from the Architecture group
- Missing basic functionality in the EBW wallets, and in the trust infrastructure that need to be provided by WG4:
 - mutual identification & consent handshake: <https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/blob/main/rulebooks/rb-base/holder-authorization-handshake.md>
 - basic verification of attestations rulebook: <https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/blob/main/rulebooks/rb-base/verifier-base-verification.md>
 - Related to the implementation of the following issues created by BU1 in March 2026 based on the User Requirements document reviewed by BU1 participants:
 - Protect confidential attestations in a EBW according to legislation and own business policies

- [Attestation issuing without any EBW owner end user interaction](#)

Currently the European Business Wallet Relying Party role is defined in the Business Wallet Regulation draft. There is no European Business Wallet component defined.

Some of the participants assume that the EBW Relying Party will use a EBW other participants assume that a EBW Relying Party component will be used. WE BUILD needs to decide if:

- a) European Business Wallet Relying Party component will be used in BU1 and PA3
- b) If Holders need to answer Relying Party component requests for confidential data
- c) how the seller can be identified by the holder during a confidential data request

The following Architectural Design Request was created: <https://github.com/webuild-consortium/wp4-architecture/pull/205>.

This ADR proposal is not yet fully aligned within the scenario group and the defined workflows and reflects the view of a subgroup within Scenario 1. The pilot will rely on the solution defined together with WG4.

Without a solution for the above mentioned barriers we will not be able to present confidential attestations and verify received EAAs. Therefore the MVP and also the MVP+ will be a showcase and not a demonstration of technical feasibility.

2.7 Working Assumptions

It is assumed that semantic interoperability is ensured among participants in a standardised manner including human- and machine-readable definitions. Further, it is assumed that interoperability with respect to the trust framework, protocols and formats is given by WP4.

3 Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Legal Entity selection	Company (Buyer) Initiator	Accesses the Seller's website and selects the appropriate method for data exchange to initiate the KYC process (e.g., via URI, direct integration).		
	Seller (Service Provider) Portal	The Seller Portal presents the options for connecting the Business Wallet.		
	Company (Buyer) Initiator	Select the option to connect to the business wallet (automatic or manual process).	Initiator must have access to a Business Wallet.	The connection can be established via an automatic endpoint, a pre-integrated business process in the wallet, or a manual flow (QR code/copy-paste).
Use Case specific additional data	Seller (Service Provider) Portal	The portal displays input fields to collect the specific data from the initiator.		
	Company (Buyer) Initiator	Manually enters contact data: name, surname, and email address into the Seller's portal.		An optional telephone number can also be provided.
Legal Entity Identification	Seller (Service Provider) Business Wallet	Generates a request for a set of attestations: EBWOID, EUCC, (Tax number,) VAT, Company Info, and Contact Person.		The request can be delivered automatically or encoded into a QR code for a manual scan.

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
	Company (Buyer) Business Wallet	Receives the request, and after user authorization, presents the required attestations to the Seller's wallet.	The Company's Business Wallet must hold all the requested attestations.	Mutual authentication between the wallets is performed according to the WEBUILD rulebook before data is presented.
	Seller (Service Provider) Business Wallet	Receives the attestations and performs a base verification according to the rulebook.		The verification includes checking the authenticity and integrity of the presented data.
Organisation Structure	Seller (Service Provider) Business Wallet	After verifying the initial data, it requests additional attestations based on internal policy: Ownership List and Control List.	This step is conditional, depending on the Seller's internal policy engine and risk assessment.	
	Company (Buyer) Business Wallet	Presents the Ownership List and Control List attestations to the Seller's wallet upon request.	The Company's wallet must hold the Ownership and Control List attestations.	
Additional Identifiers (MVP+)	Seller (Service Provider) Business Wallet	(MVP+ Feature) Requests additional attestations such as the LEI (Legal Entity Identifier).	This is an optional step, typically required for use cases in the financial sector.	This step is part of the MVP+ extension and not the standard MVP flow.
	Company (Buyer) Business Wallet	(MVP+ Feature) Presents the LEI attestation as requested.	The Company's wallet must hold the LEI attestation.	

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Use case specific cross check & transfer	Seller (Service Provider) Internal System	Performs a final cross-check across all the verified attestations and transfers the data to its internal IT systems.	All previous steps must be successfully completed.	
	Seller (Service Provider) Portal	Notifies the contact person (provided in the specific data step) that the onboarding was successful and displays a success notification to the initiator.		

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner name	Countries
1. User of EBW	Robert Bosch GmbH	DE+NL
	SBB - Swiss Federal Railways	CH
	Deutsche Bahn Cargo AG	DE
	voestalpine Rail Technology GmbH	AT
	Orange	FR
	SICPA	ES
	Leone SRL	IT
2. Authentic Sources	Bundesanzeiger Verlag	DE
	KVK	NL
	Dutch Tax Agency	NL
	DATEV	DE
	Infogreffe (Docaposte)	FR
	Infocamere	IT
	CT Notariado	ES
3. Relying Party	Deutsche Bank AG	DE
	Orange	FR
	Robert Bosch GmbH	NL
	SBB - Swiss Federal Railways	CH
	Deutsche Bahn Cargo AG	DE
	voestalpine Rail Technology GmbH	AT

4.2 Additional roles and partners

Primary role	UC partner Name	Countries	Wallet
3. EBW provider	Spherity GmbH	DE	BW
	Procivis GmbH	AT	BW
	Credenco B.V.	NL	BW
4. PID Provider			
5. Trusted list registrar			
6. QEAA provider	Procivis (interim, technology for QTSP)	AT	BW
	Spherity (interim, technology for QTSP)	DE	BW
7. Pub-EAA provider	Bundesanzeiger Verlag	DE	BW
	KVK	NL	BW
	Dutch Tax Agency	NL	BW
	DATEV	DE	BW
	Infogreffe (Docaposte)	FR	BW
8. EAA provider	can be any of the above parties, refer to chapter 4.1	EU	BW
9. QES provider	n/a for our workstream/scenarios	-	-

4.3 Target country combinations

Relying Party country (Service Provide r)	Holder (& authentic source) country (customer)							
		AT	DE	FR	NL	CH	ES	IT
	AT		X		X	X		
	DE	X			X	X	X	X
	FR		X		X	X		
	NL		X			X	X	X
	CH	X	X		X			
	ES							
	IT							

4.4 Requirements

The section 2.6 () contains requirements related to WG4 that need to be implemented or rejected.

5 Attestations

5.1 Introduction

This section summarises the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For Countries	Requirements
EBWOID	European Business Wallet Owner Identification Data	WP4	DE / AT / CH / FR /NL / IT / ES	
EUCC	European Company Certificate	BU2	DE / AT / CH / FR /NL / IT / ES	
Tax number	Tax number of a legal person (non sole trader)	PA1	DE / AT / CH / FR /NL / IT / ES	
VAT	Tax number of a legal person (non sole trader)	BU3	DE / AT / CH / FR /NL / IT / ES	
Ownership List	Direct owners of the company	PA3	DE / AT / CH / FR /NL / IT / ES	
Control List	Control structure of the company	PA3	DE / AT / CH / FR /NL / IT / ES	
LEI (MVP+)	Legal Entity Identifier	BU1 Scenario 2	DE / AT / CH / FR /NL / IT / ES	

Attestation name	Short description	To be provided by	For Countries	Requirements
WUA (MVP+)	Wallet Unit Attestation	WP4	DE / AT / CH / FR / NL / IT / ES	According to EU Business Wallet regulation Article 14/2/b"...Wallet units shall enable authentication and validation of the wallet unit components by presenting the wallet unit attestations...

5.3 Created attestations in the scenario

Attestation name	Short description	For Countries	Applicable domain standards
Contact Person	Properties of a contact person responsible for the business relation	Self-attestation	
Company Info		Self-attestation	

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organisational/technical requirements for each role in the scenario.

Primary role	Specific requirement
User of EUDI Wallet	a.
	b.
	c.
Authentic sources	a.
	b.
	c.
Relying Party	a. Some holders have defined a requirement that Relying Party requests MUST use an EBW and not a Relying Party Component (e.g. used to access EUDI Wallets for natural person) when requesting confidential data from a buyer's/holder's EBW
	b.
	c.
Intermediary	a.
	b.
	c.
EUDI Wallet provider	a.
	b.
	c.
PID Provider	a.
	b.
	c.
Trusted list registrar	a.
	b.
	c.
QEAA provider	a.
	b.
	c.
Pub-EAA provider	a.
	b.
	c.
EAA provider	a.
	b.
	c.
QES provider	a.
	b.
	c.

The following slide explains why some Buyer EBW Wallets will not present confidential data requested by a Seller Relying Party Component.



EBWOID and EBW trustworthiness compared to Relying Party SW with Access Certificate from Holder perspective, who has to present confidential attestations

Criteria	EBWOID issued to an EBW owner		Access Certificate issued to a proprietary Relying Party software	
	Rating	Comment	Rating	Comment
Cryptographic possession trust	+	Potentially significantly stronger due to wallet-controlled and hardware-backed keys	-	Weaker if private keys are exportable or software-managed
Anti-cloning protection	+	Strong wallet unit attestation and secure-element binding can prevent cloning	-	Private key duplication may allow identity cloning
Runtime integrity	+	WUA can provide attested runtime integrity and secure execution guarantees	-	Typically does not prove runtime or software-instance integrity
Key custody assurance	+	Strong key custody through wallet binding and non-exportable keys	-	Depends on RP operational controls and HSM usage
Execution trust	+	High trust through attested cryptographic runtime identity	-	Mainly proves organizational ownership of key
Legal authorization	-	Requires complementary ecosystem governance, that needs to be established	+	Strong organizational authorization and formal onboarding
Ecosystem governance	+	Based on the EBWOID rulebook; highest legal value it contains PID for legal entities (according to eIDAS2.0)	+	Strong support for ecosystem governance and federation

Attested execution identity through EBWOID bound to the EBW is more important than static organizational identity through Access Certificate issued to a legal entity.



Illustration 1: Evaluation of trust levels

Annex 2 – MVP partner overview

Remark: The following list is a snapshot of the MVP partners as of 2026-06-19. Due to the dynamic nature this might have already become more complete by the day after.

BU1 KYC	Attestation type ¹	EBWOID (LPID)	EUCC	TAX NR (company)	VAT	Contact Person	Company Info	LEI (MVP+)	Owner List	Control List
		Business Register	Business Register / BRIS		Self-issued ²	EAA- Attestation	EAA- Attestation		EAA- Attestation ³	EAA- Attestation
Holder (EUBW)	Bosch (DE)	Bundes- anzeiger	Bundes- anzeiger		National register ⁴	Self-issued	Self-issued	Bundes- anzeiger / KVK	Self-issued	Self-issued
	Bosch (NL)	KVK	KVK	Tax admi- nistration (NL)	Tax admi- nistration (NL)	Self-issued	Self-issued	Bundes- anzeiger / KVK	Self-issued	Self-issued
	SBB (CH)	Bundes- anzeiger	Bundes- anzeiger		Self-issued (maybe Bundes- anzeiger)	Self-issued	Self-issued	Bundes- anzeiger / KVK	Self-issued or Bundes- anzeiger	Self-issued or Bundes- anzeiger
	Voestalpine (AT)	Bundes- anzeiger	Bundes- anzeiger		Self-issued (maybe Bundes- anzeiger)	Self-issued	Self-issued	Bundes- anzeiger / KVK	Self-issued or Bundes- anzeiger	Self-issued or Bundes- anzeiger

¹Issuer: see XLS file

²Optionally National Register or Tax Administration

³Type: QEAA (!)

⁴Ministry of Finance; currently under discussion with Bundesanzeiger and MoF

BU1 KYC	Attestation type ¹	EBWOID (LPID)	EUCC	TAX NR (company)	VAT	Contact Person	Company Info	LEI (MVP+)	Owner List	Control List
		Business Register	Business Register / BRIS		Self-issued ²	EAA- Attestation	EAA- Attestation		EAA- Attestation ³	EAA- Attestation
	Deutsche Bahn Cargo (DE)	Bundes- anzeiger	Bundes- anzeiger		Self-issued (maybe Bundes- anzeiger)	Self-issued	Self-issued	Bundes- anzeiger / KVK	Self-issued or Bundes- anzeiger	Self-issued or Bundes- anzeiger
	Orange (FR)	Infogreffe	Infogreffe		To be clarified	Self-issued	Self-issued	Bundes- anzeiger / KVK	Self-issued	Self-issued
	SICPA (ES)	CT Notariado	CT Notariado		To be clarified	Self-issued	Self-issued	Bundes- anzeiger / KVK	Self-issued	Self-issued

WE BUILD consortium

Specification Scenario 2 – KYS (B2B vertical)

WP2 – BU1

Date : 19.06.2026
Version : 1.0
Status : final

Table of Contents

1 Introduction.....	4
1.1 <i>Objectives of this document</i>	4
1.1.1 Requirements Status by Project Phase	4
1.1.2 Most important open topics	4
1.1.3 Most relevant points for future revisions	4
1.2 <i>Scenario introduction</i>	4
2 Scenario specification.....	6
2.1 <i>Introduction</i>	6
2.2 <i>Scenario pre-conditions</i>	6
2.2.1 MVP Restrictions	7
2.2.2 Planned MVP+ Extension	8
2.3 <i>Issuing the required attestations</i>	8
2.4 <i>Scenario main flow</i>	9
2.4.1 Service Selection & Business Wallet selection.....	13
2.4.2 Use Case specific additional data	13
2.4.3 Legal Entity Identification	14
2.4.4 Payment Information	15
2.4.5 Organisation Structure	16
2.4.6 Additional Identifiers (MVP+)	17
2.4.7 UBO (MVP+).....	18
2.4.8 Social Security Attestation (MVP+).....	19
2.4.9 Fraud&Sanction (MVP+).....	19
2.4.10 ESG Certificate (MVP+)	20
2.4.11 Use case specific cross check & transfer in the internal system.....	21
2.5 <i>Scenario additional flows</i>	22
2.6 <i>Challenges and barriers</i>	22
2.7 <i>Working Assumptions</i>	23
3 Detailed scenario flow	24
4 Roles and participants.....	27
4.1 <i>Scenario roles and participants</i>	27
4.2 <i>Additional roles and partners</i>	27
4.3 <i>Target country combinations</i>	28
4.4 <i>Requirements</i>	28
5 Attestations	29
5.1 <i>Introduction</i>	29
5.2 <i>Attestations to be provided by other UCs/WGs/scenarios</i>	29
5.3 <i>Created attestations in the scenario</i>	30

Annex 1 – Requirements for scenario roles 31

Annex 2 – MVP partner overview 32

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 2, as part of use case BU1 in Work Package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.1.1 Requirements Status by Project Phase

MVP Requirements Status	MVP+ Requirements Status	General Comments
1.0	0.7	MVP: final MVP+: ongoing

1.1.2 Most important open topics

Topic	Description	Responsible	Solved

1.1.3 Most relevant points for future revisions

Review Item	Description
Update Process Flows: Chapter 2	In chapter 2 is written "No attestations are issued to or presented from an EUDI Wallet". The EUDI Wallet should be removed in all diagrams.

1.2 Scenario introduction

The BU1 scenario 2 use case aims to redefine a core flow for European businesses. The objective of this use case is to demonstrate the applicability of the EU Business Wallet for companies in the process of Know Your Supplier (KYS) due diligence with regard to fulfil regulatory obligations as well as business obligations in general. Digitising KYS processes improves trust, transparency, and compliance while significantly reducing onboarding time and cost - especially in cross-border contexts.

Company A (country A) wants to enter into a business relationship with another company B (Country B) and wants to become a supplier of company B.

A legal representative (initiator) of company A is initiating the process of issuance and presentation of required KYS attestations. Authorisation is out of scope of this scenario.

A process based on verifiable, interoperable, and reusable organisational attestations has the following benefits for the market:

- Faster establishment of cross-border business relationships
- Reduced fraud and compliance risks
- Increased efficiency and competitiveness for European enterprises
- A resilient and trustworthy digital single market

The scenario is based on the following documentation:

1. **BU1 Stock Taking document:**

<https://portal.webuildconsortium.eu/group/bu1-kyskykybdd/files?mid=5921&fid%5B0%5D=11&fid%5B1%5D=12&fid%5B2%5D=4188>

2. **WE BUILD Architecture & Integration Blueprint:**

<https://portal.webuildconsortium.eu/topic/d41-architecture-integration-blueprint-reference-document>

3. **EBWOID Data schemas & Issuance rulebooks:**

<https://portal.webuildconsortium.eu/topic/ms14-pid-ebwoid-data-schema-issuance-rulebook>

2 Scenario specification

2.1 Introduction

This scenario pilots the onboarding process for enterprise supplier which provide goods or services. To satisfy standard due diligence requirements, the service provider mandates that the customer present a specific set of digital attestations to verify their corporate identity.

As MVP within the BU1 (KYS/KYC/KYB/DD) use case, this scenario is conducted **exclusively using a European Business Wallet (EBW)**.

- The **Business Wallet** acts as the holder of attestations
- Natural persons **act on behalf of the organisation**; their personal identity proofing is not part of this scenario.
- No attestations are issued to or presented from an EUDI Wallet

2.2 Scenario pre-conditions

To ensure the successful execution of this scenario, the following entities and technical frameworks must be active and accessible:

- **Established EBWOID Issuer and EU Business Wallet Provider:** The legal entity must have access to a European Business Wallet (EBW) as defined in the Architecture & Integration blueprint. This wallet must be issued by a recognised provider, active and initialised with the required Business Wallet Owner Identification Data (EBWOID) to uniquely identify the business in a digital context.
- **Availability of Specific Digital Attestations:** The business must have successfully requested and stored the following credentials within their wallet:
 - EBWOID
 - EUCC
 - Tax number
 - VAT
 - CompanyInfo

- ContactPerson
- OwnershipList
- ControllList
- SanctionList (MVP+)
- UBO (MVP+)
- ESG (MVP+)
- DUNS or GS1 GLN or LEI (MVP+)
- PaymentTerms
- SiteAttestation (MVP+)
- IBAN-OV Attestation
- Social Security Attestation (MVP+)
- WUA (MVP+)
- **Harmonised Trust Framework for EAA Verification:** A functional Electronic Attestation of Attributes (EAA) verification layer must be operational. This relies on a harmonized trust framework that allows the Verifier to instantly cryptographically validate the authenticity and integrity of the data provided by the Business Wallet.
- **Mutual authentication & selection of the business wallet:** This is required in order to initiate the KYS flow and shall follow the WE BUILD-Blueprint as well as available technological options within BU1 Scenario 2.

2.2.1 MVP Restrictions

- **Reduced Verification & Trust Reliance:** Neither supplier nor buyer wallets perform full verification of attestation issuers, wallet integrity, or attestation binding.
If EAA providers are included in the WE BUILD specific trust lists and the Wallet Provider support the WE BUILD trust lists then EAA issuer verification can be demonstrated. However this solution can not be used after WE BUILD ends. The MS have explained that only QTSPs can be included in the TLOL, also due

to scalability reasons. Therefore, it is no real solution for EAA provider it is only a showcase.

Implication: The system relies on assumed trust rather than cryptographic validation, posing risks in high-assurance scenarios.

- **Limited Mutual Identification:** Supplier and buyer wallets lack robust features for securely identifying each other. The supplier wallet does not provide the attestations that allow the buyer wallet to identify the supplier. The verifierInfo object including the EBWOID and WUA of the supplier wallet is not provided when the presentation request is created. The corresponding verifierInfo object is not defined yet.

Implication: Advanced peer-to-peer identification and consent workflows using attested identities and wallet unit attestations are not yet supported.

- **Process & Risk Simplifications:** The MVP assumes all suppliers are low/medium risk, executes processes sequentially, and lacks cross-attestation checks or internal system integration.

Implication: Limits handling of complex risk scenarios, data consistency, and leveraging attested data for broader business intelligence.

- **Confidential Data Restrictions:** Current EBW versions cannot securely present highly confidential attestations due to missing security configurations.

Implication: Restricts use cases involving sensitive data within the MVP and requires careful management of data exposure.

2.2.2 Planned MVP+ Extension

- If the EBW wallet and trust infrastructure limitations documented in the chapter 2.6 () are removed then the above mentioned limitations will not apply to the MVP+
- The process will be still executed in one step (more steps are not required)
- Additionally support for Additional Identifiers,UBO , Fraud&Sanction, Social Security Attestation (MVP+)

2.3 Issuing the required attestations

Before the KYS process can be executed, the suppliers EBW must be provisioned with the required attestations. These attestations are categorized into two primary types:

- a. **Externally Issued Attestations:** many of these attestations represent assertions made by authoritative external entities. These may include public sector bodies (such as official business registers) or private entities (such as EAA providers). Users can request these attestations either through the respective issuer's external portal or directly via the EBW, which may feature a pre-configured set of attestation requests for supported issuers.
- b. **Self-Issued Attestations:** certain information cannot be validated by external entities and must be asserted directly by the EBW owner. These attestations are generated using a local issuer component, which is ideally integrated natively within the economic operator's EBW¹.

A current overview with regard to the issued attestations during BU1 KYS MVP can be found in . *The exact process of issuing attestations, however, belongs to the rulebooks and is not part of this document.*

2.4 Scenario main flow

The onboarding journey begins when a person navigates to the buyer's website and selects the desired service. To facilitate clear communication

- **Block1:** the initiator selects the appropriate method for the data exchange between the wallet and the respective business partner. This can be done via URI, a direct integration to the Wallet or endpoint retrieval.
- **Block2:** the initiator provides their contact details, ensuring that all subsequent status updates and results reach the correct stakeholder.

In order to be flexible, the process is built using building blocks Block1 and Block2 which can be adapted for each company requirements. In the MVP we will demonstrate the order specified above (B1 then B2).

With the endpoint identified, a critical security handshake occurs: the Supplier's and the Buyer's Business Wallet perform mutual identification. This ensures a trusted connection before any sensitive data moves. Upon successful verification, the wallet shares the base business data.

The process then moves into a dynamic phase where the provider requests additional application-specific attestations. Depending on the complexity of the service, this exchange may iterate multiple times to satisfy all compliance

¹For further details please refer to EBW regulation Art. 6

requirements. Finally, once all requested attestations are successfully validated, the data is integrated into internal systems for processing, and the applicant is promptly notified of the result.

The following figure depicts an overview of the process:

Scenario 1 & 2: Specification

KYS Flow

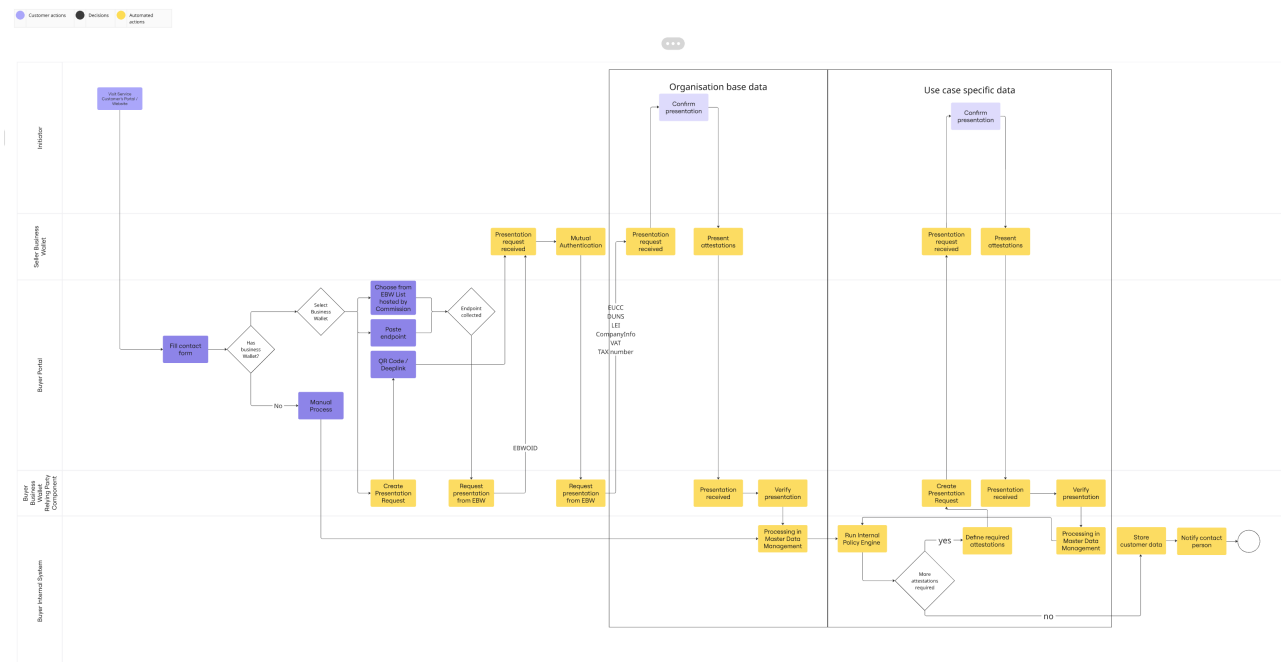


Figure 1: KYS Flow

The required actors and software systems for the flow detailed in the following interaction diagrams are:

- Software systems owned by the supplier legal entity
 - Buyer Business Wallet: EBW of the supplier acting primarily in the holder role during this workflow.
- Software systems owned by the buyer legal entity
 - Buyer Business Wallet Relying Party Component or buyer Business Wallet: EBW wallet or Wallet Relying Party Component of the buyer that acts in the EBW Relying Party.
 - Buyer Portal: Web application owned by the buyer legal entity that acts as a frontend for customer employees

- Buyer Internal System: ICT systems owned by the buyer , into which the presented data is transferred, e.g. enterprise relationship management system or supplier master data management system.
- Software systems owned by the (Q)EAA providers
 - (Q)EAA provider revocation service: Revocation service for the (Q)EAA provider with unified revocation interface toward the EBW also for QEAs
- Software systems owned by the EBWOID provider
 - EBWOID revocation service: Revocation service for the EBWOID
- Software systems for which the national Supervisory Body is responsible
 - Trust List that are part of the TLOL and included the EBWOID provider certificates
- Software systems for which the WalletProvider Provider is responsible
 - Wallet Unit Attestation (WUA) revocation service: Revocation service for the WUA
- Software systems for which the EAA Provider is responsible
 - EAA revocation service: Revocation service for the EAAs including the self issued EAAs

The following diagram provides an overview of the end-to-end process for MVP and MVP+

Figure 2: [Workflow Overview](#)

Notes: the block specific for the MVP+ are marked with green background in the diagram

The MVP and MVP+ pre-requisites for the scenario are shown in the following interaction diagram:

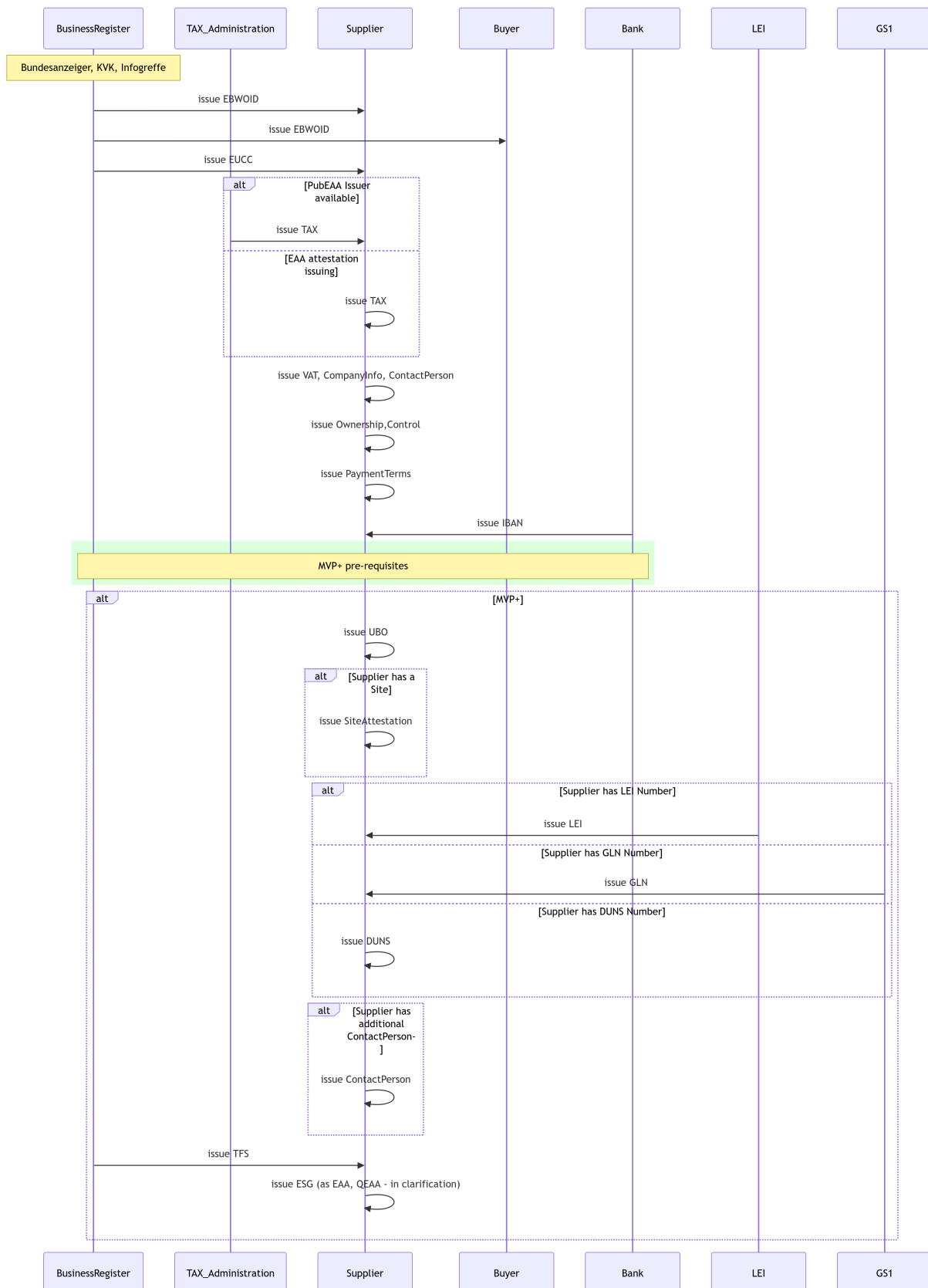


Figure 3: Prerequisites

Notes: the block specific for the MVP+ are marked in the diagram

The buyers wallet needs all the attestations requested by the supplier in his wallet.

The supplier needs to provide all the attestations needed by the buyer during mutual identification.

In the following sections, the building blocks of the process are defined in detail.

2.4.1 Service Selection & Business Wallet selection

To ensure seamless communication, the initiator select the Business Wallet

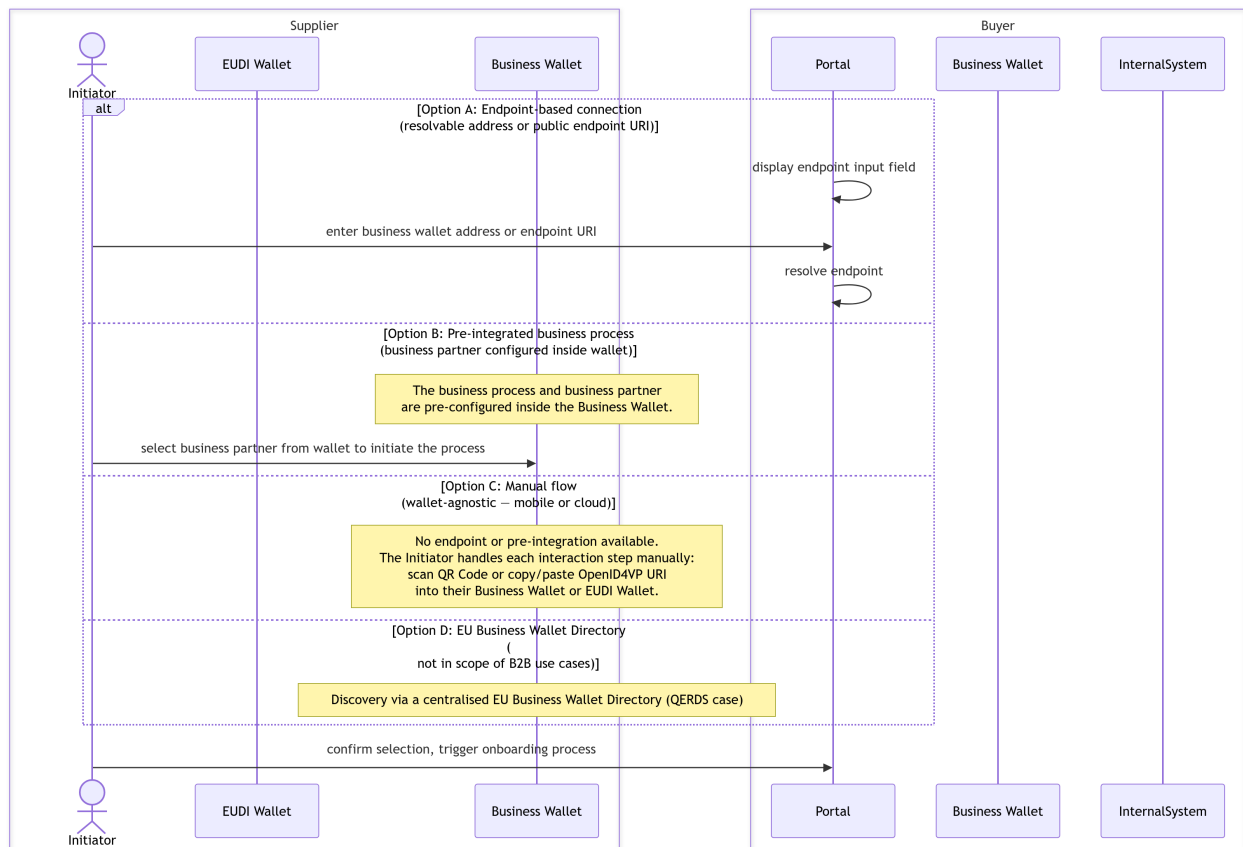


Figure 4: Legal Entity Selection

2.4.2 Use Case specific additional data

The following additional info need to be manually inserted per request for a complete KYC flow (as input):

- Person contact data : name, surname, email address
- Optional telephone

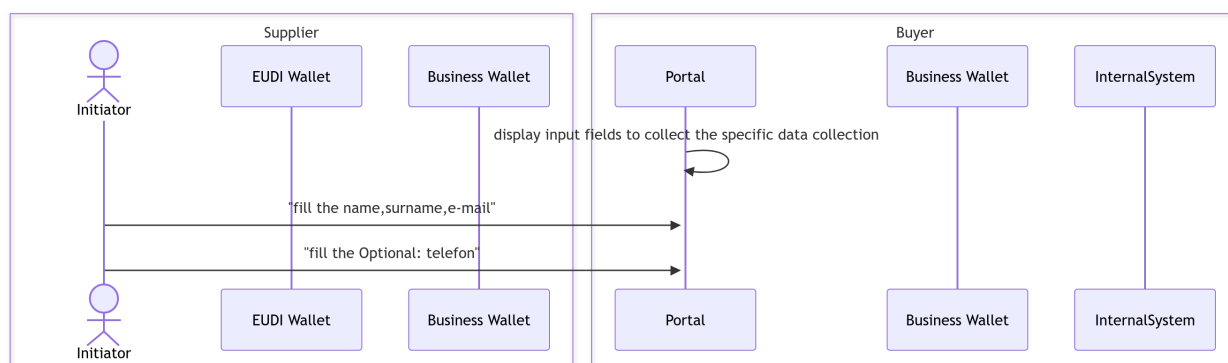


Figure 5: Use Case Specific Data Collection

2.4.3 Legal Entity Identification

The following interaction diagram describes the interaction between supplier and buyers organisation starting with the supplier portal request to generate a proof request for several attestations which should be presented by the supplier's wallet. The step ends after the verification of the presented attestations according to the attestation rulebooks.

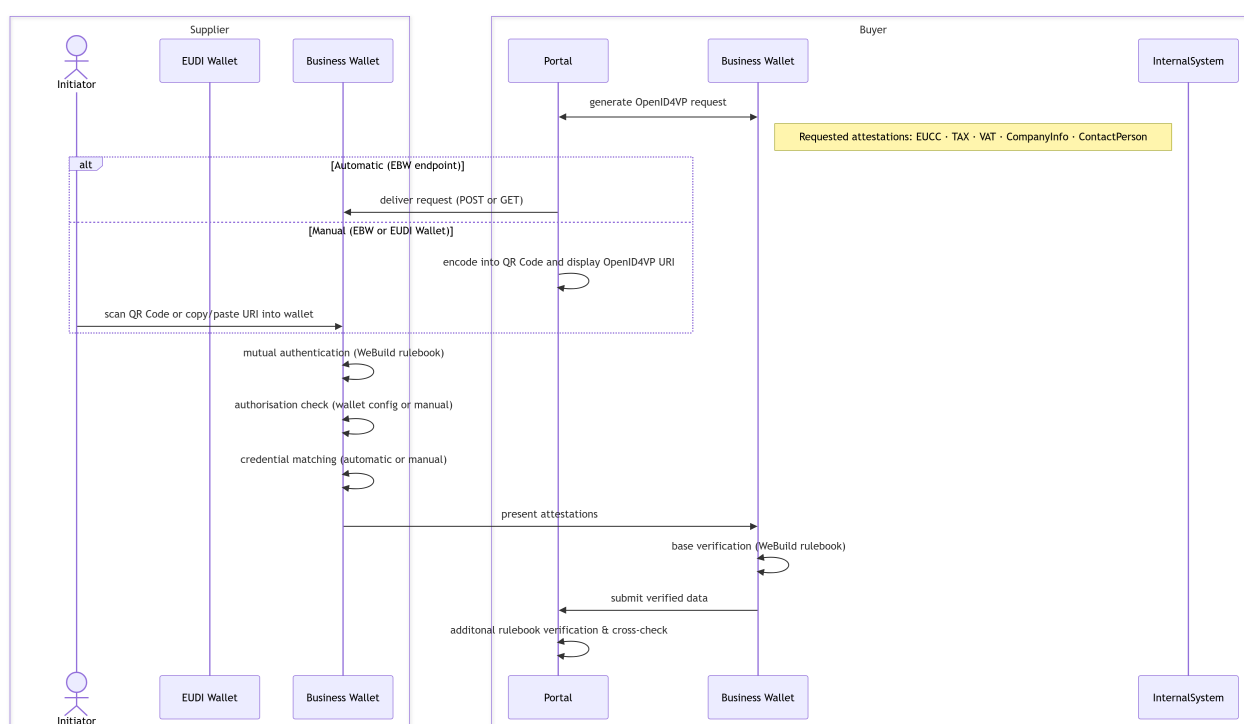


Figure 6: Legal Entity Identification

Before any sensitive data is exchanged, a secure handshake occurs. The Supplier Business Wallet and the Buyers Business Wallet perform mutual identification to verify the identity and integrity of both parties.

The mutual identification step is defined and detailed in the following rulebook, that will be reviewed by the architecture group: <holder-authorization-handshake.md>

After successful identification of the requesting buyer wallet, the requested company base data is presented by the supplier wallet:

- EBWOID
- EUCC
- Tax number
- VAT
- Company Info
- ContactPerson

The Wallet Unit Attestation may also be requested by the buyer.

According to EU Business Wallet regulation Article 14/2/b "[...] Wallet units shall enable authentication and validation of the Wallet unit components by presenting the Wallet unit attestations. [...]"

The WUA revocation status can be used by the supplier to avoid requesting data from revoked EBWs (e.g. due to compromise).

For each presented attestation the basic verification steps are performed by the supplier wallet.

The basic verification steps are described in the following rulebook: [verifier-base-verification.md#42-relying-party-obligations](#)

2.4.4 Payment Information

After verification of the base data attestation and running the internal policy engine, it may be necessary, depending on the use case, that additional information is retrieved, in order to finalise the onboarding and set up a contractual relationship.

- Payment Terms
- IBAN

The interaction diagram and the performed steps are similar to the steps described in section 2.4.3 :

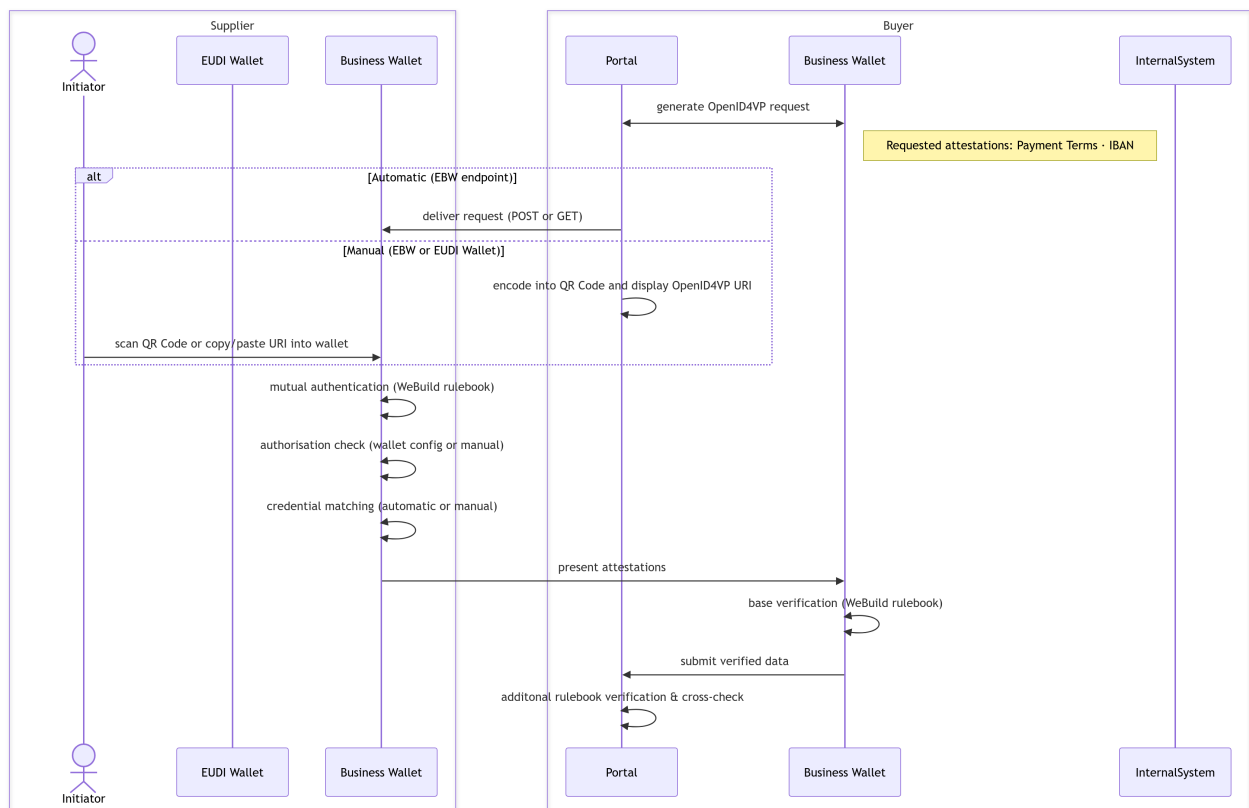


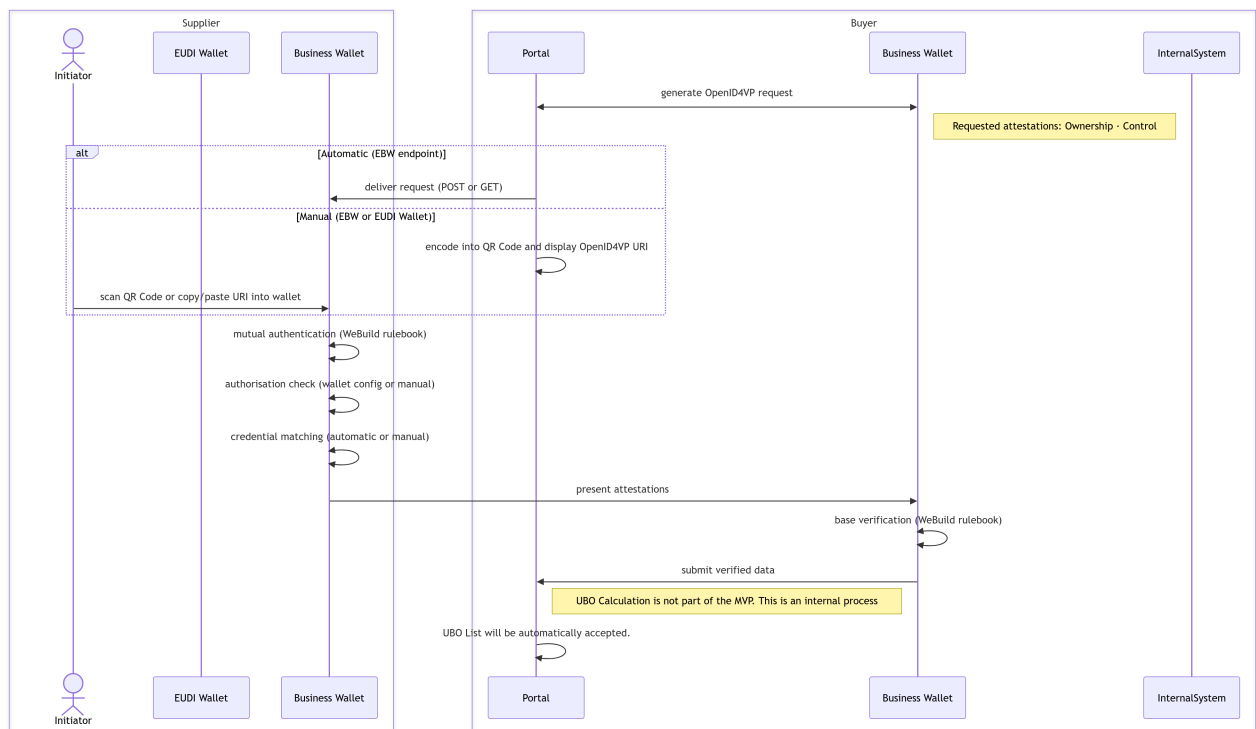
Figure 7: Payment Information

2.4.5 Organisation Structure

After verification of the base data attestation and running the internal policy engine, it may be necessary, depending on the use case, that additional information is retrieved, in order to finalise the onboarding and set up a contractual relationship.

- OwnershipList
- ControllList

The interaction diagram and the performed steps are similar to the steps described in section 2.4.3 :



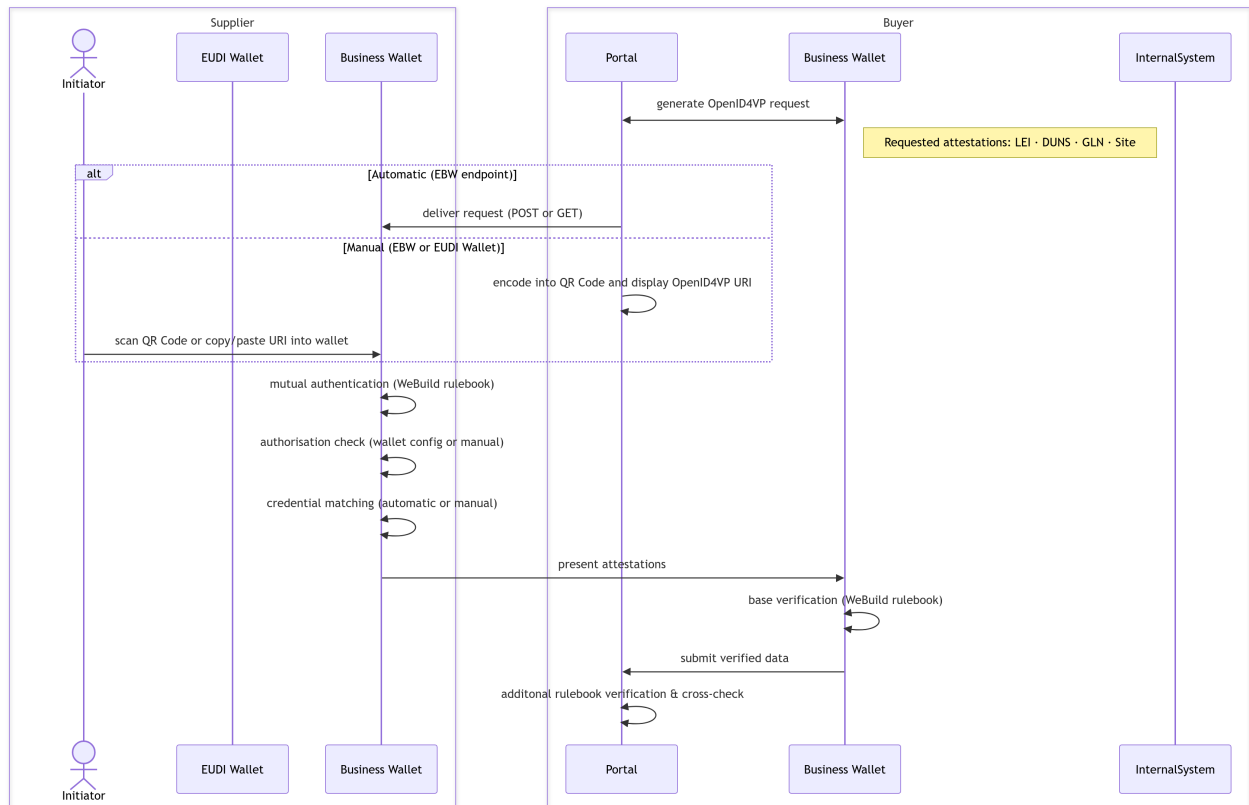


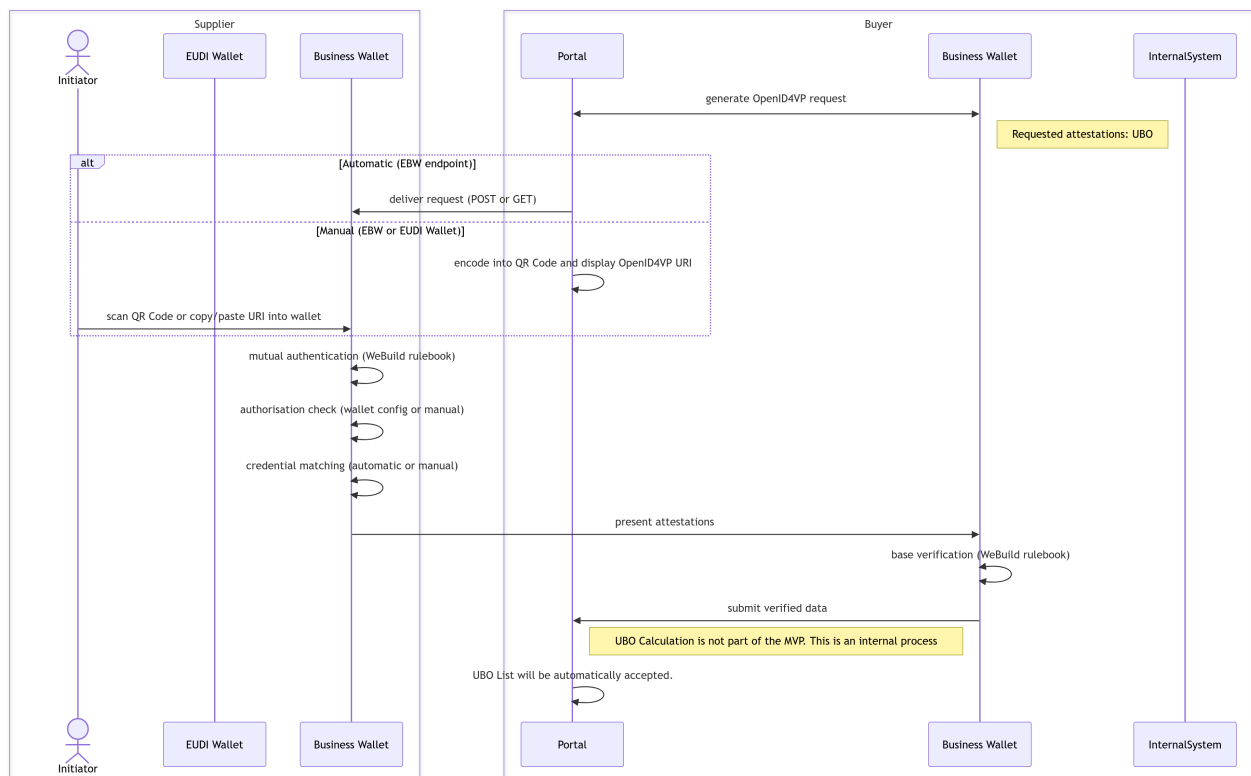
Figure 9: Additional Identifiers

2.4.7 UBO (MVP+)

After verification of the base data attestation and running the internal policy engine, it may be necessary, depending on the use case, that additional information is retrieved, in order to finalise the onboarding and set up a contractual relationship.

- UBO

The interaction diagram and the performed steps are similar to the steps described in section 2.4.3 :





After verification of the base data attestation and running the internal policy engine, it may be necessary, depending on the use case, that additional information is retrieved, in order to finalise the onboarding and set up a contractual relationship.

- The interaction diagram and the performed steps are similar to the steps described in section 2.4.3 :

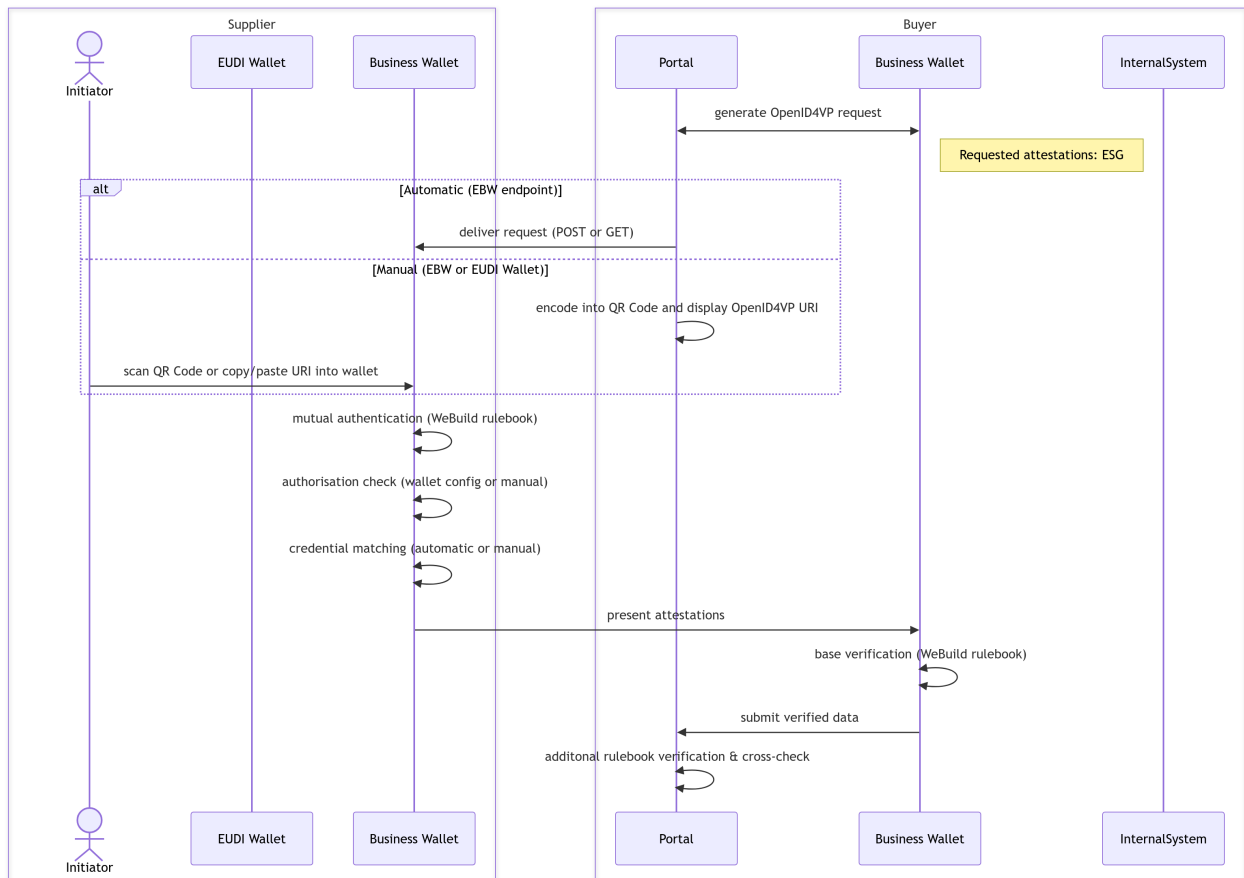


Figure 12: ESG

2.4.11 Use case specific cross check & transfer in the internal system

After successful validation, the data is transferred to the internal IT systems of the relying party for further processing and the contact person is notified.

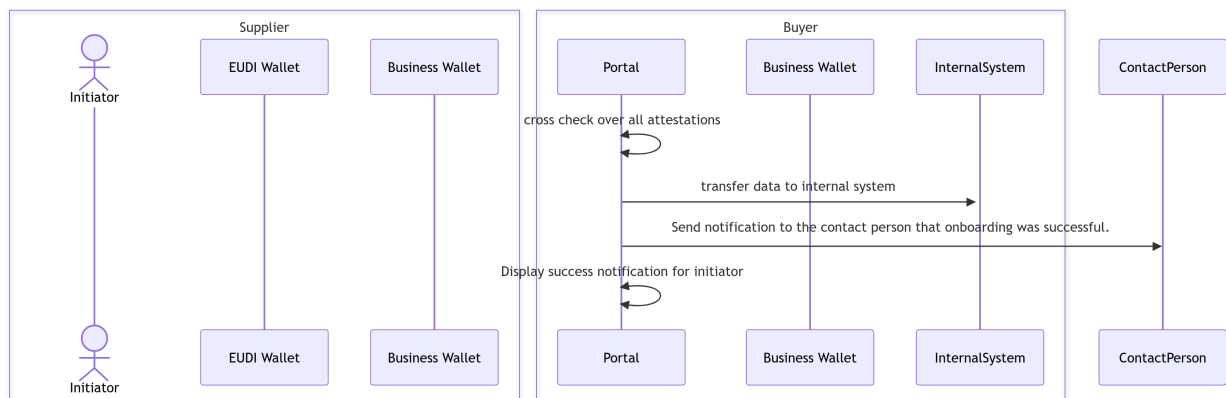


Figure 13: Cross Check

2.5 Scenario additional flows

Flow	Short description
Variations	
- Tax information available from authentic source	If an authentic source is available for the country of the customer, tax related attestations shall be issued by these.
- Tax information not available from authentic source	If no authentic source is available for the country of the customer, the related attestations shall be issued as a self-issued attestation.
- LEI for financial applications	If the context is in the financial sector, an LEI attestation shall be requested by the service provider.
- User consent	In this variation, the a Business Wallet user gives consent to present data with the relying party.
- Automated consent	In this variation, the Business Wallet is configured to give consent based on a policy engine.

2.6 Challenges and barriers

The scenario depends on multiple architecture decisions such as the implementation of mutual identification, consent management in the business wallet, EAA verification, and attestation chaining. Due to the complexity and number of attestations required within the scenario, semantic alignment is paramount to achieve interoperability between participants and between use cases sharing attestations. Therefore, a mechanism for appropriately defining semantics is required.

The above restrictions described in “MVP and MVP + Restrictions” are due to:

- 1 Missing agreement to the ADR EAA provider identity verification based on chaining and TLOL that is needed from the Architecture group.
- 2 Missing basic functionality in the EBW wallets, and in the trust infrastructure that need to be provided by WG4:
 - mutual identification & consent handshake: <https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/blob/main/rulebooks/rb-base/holder-authorization-handshake.md>
 - basic verification of attestations rulebook: <https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/blob/main/rulebooks/rb-base/verifier-base-verification.md>

- Related the implementation of the following issues created by BU1 in March 2026 based on the User Requirements document reviewed by BU1 participants:

- Protect confidential attestations in a EBW according to legislation and own business policies
- [Attestation issuing without any EBW owner end user interaction](#)

3 Currently the European Business Wallet Relying Party role is defined in the Business Wallet Regulation draft. There is no European Business Wallet component defined.

Some of the participants assume that the EBW Relying Party will use a EBW other participants assume that a EBW Relying Party component will be used. WE BUILD needs to decide if:

- a) European Business Wallet Relying Party components will be used in BU1 and PA3
- b) If holders need to answer Relying Party component requests for confidential data
- c) how the supplier can be identified by the holder during a confidential data request

The following Architectural Design Request was created:

<https://github.com/webuild-consortium/wp4-architecture/pull/205>.

- The ADR is also included in the Annex of this document.
- The ADR proposal is not yet fully aligned within the scenario group and the defined workflows reflect the view of a subgroup within Scenario 1. The pilot will rely on the solution defined together with WG4.

Without a solution for the above mentioned barriers we will not be able to present confidential attestations and verify received EAAs. Therefore the MVP and also the MVP+ will be a showcase and not a demonstration of technical feasibility.

2.7 Working Assumptions

It is assumed that semantic interoperability is ensured among participants in a standardised manner including human- and machine-readable definitions. Further, it

is assumed that interoperability with respect to the trust framework, protocols and formats is given by WP4.

3 Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Legal Entity selection	Supplier (Holder) Initiator	Accesses the Buyer's website and selects the appropriate method for data exchange to initiate the KYS process.		
	Buyer (Verifier) Portal	The Buyer Portal presents the options for connecting the Business Wallet.		
	Supplier (Holder) Initiator	Selects the option to connect to the business wallet (automatic or manual process).	Initiator must have access to a Business Wallet.	The connection can be established via an automatic endpoint, a pre- integrated business process in the wallet, or a manual flow (QR code/copy- paste).
Use Case specific additional data	Buyer (Verifier) Portal	The portal displays input fields to collect the specific data from the initiator.		
	Supplier (Holder) Initiator	Manually enters contact data: name, surname, and email address into the Buyer's portal.		An optional telephone number can also be provided.
Legal Entity Identification	Buyer (Verifier) Business Wallet	Generates a request for a set of attestations: EUCC, Tax number, VAT, Company Info, and Contact Person.		The request can be delivered automaticall y or encoded into a QR code for a manual scan.

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
	Supplier (Holder) Business Wallet	Receives the request, and after user authorization, presents the required attestations to the Buyer's wallet.	The Supplier's Business Wallet must hold all the requested attestations.	Mutual authentication between the wallets is performed according to the WeBuild rulebook before data is presented.
	Buyer (Verifier) Business Wallet	Receives the attestations and performs a base verification according to the rulebook.		The verification includes checking the authenticity and integrity of the presented data.
Organisation Structure	Buyer (Verifier) Business Wallet	After verifying the initial data, requests additional attestations based on internal policy: Ownership List and Control List.	This step is conditional, depending on the Buyer's internal policy engine and risk assessment.	
	Supplier (Holder) Business Wallet	Presents the Ownership List and Control List attestations to the Buyer's wallet upon request.	The Supplier's wallet must hold the Ownership and Control List attestations.	
Additional Identifiers (MVP+)	Buyer (Verifier) Business Wallet	(MVP+ Feature) Requests additional attestations such as the LEI (Legal Entity Identifier).	This is an optional step, typically required for use cases in the financial sector.	This step is part of the MVP+ extension and not the standard MVP flow.
	Supplier (Holder) Business Wallet	(MVP+ Feature) Presents the LEI attestation as requested.	The Supplier's wallet must hold the LEI attestation.	

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
UBO (MVP+)	Buyer (Verifier) Business Wallet	(MVP+ Feature) Requests the UBO (Ultimate Beneficial Owner) attestation.	Necessary for regulatory compliance and risk assessment.	
	Supplier (Holder) Business Wallet	(MVP+ Feature) Presents the UBO attestation upon request.	The Supplier's wallet must hold the UBO attestation.	
Fraud & Sanction (MVP+)	Buyer (Verifier) Business Wallet	(MVP+ Feature) Requests attestations for fraud and sanctions screening.	Dependent on risk assessment of the submitted data.	
	Supplier (Holder) Business Wallet	(MVP+ Feature) Presents the required fraud and sanction- related attestations.	The Supplier's wallet must hold the requested attestations.	
ESG (MVP+)	Buyer (Verifier) Business Wallet	(MVP+ Feature) Requests ESG (Environmental, Social, and Governance) certificates.	Based on the Buyer's internal policy to assess the supplier's ESG credentials.	
	Supplier (Holder) Business Wallet	(MVP+ Feature) Presents the ESG certificates as requested.	The Supplier's wallet must hold the ESG certificates.	
Use case specific cross check & transfer	Buyer (Verifier) Internal System	Performs a final cross- check across all the verified attestations and transfers the data to its internal IT systems.	All previous steps must be successfully completed.	
	Buyer (Verifier) Portal	Notifies the contact person (provided in the specific data step) that the onboarding was successful and displays a success notification to the initiator.		

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of EBW	Robert Bosch GmbH	DE+NL
	SBB - Swiss Federal Railways	CH
	Deutsche Bahn Cargo AG	DE
	voestalpine Rail Technology GmbH	AT
	Orange	FR
2. Authentic Sources	Bundesanzeiger Verlag	DE
	KVK	NL
	Dutch Tax Agency	NL
	DATEV	DE
	Infogreffe (Docaposte)	FR
	Infocamere	IT
	GS1 Switzerland	CH
3. Relying Party	La Post	FR
	Orange	FR
	Robert Bosch GmbH	NL
	SBB - Swiss Federal Railways	CH
	Deutsche Bahn Cargo AG	DE
	voestalpine Rail Technology GmbH	AT
	DFØ	NO

4.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
- EBW provider	Spherity GmbH	DE	BW
	Procivis GmbH	AT	BW
	Credenco B.V.	NL	BW
- PID provider			
- Trusted list registrar			
- QEAA provider	Procivis (interim, technology for QTSP)	NL	BW
	Spherity (interim, technology for QTSP)	DE	BW
- Pub-EAA provider	Bundesanzeiger-Verlag	DE	BW
	KVK	NL	BW
	Dutch Tax Agency	NL	BW
	DATEV	DE	BW
	Infogreffe (Docaposte)	FR	BW
- EAA provider	can be any of the above parties, refer to chapter 4.1	EU	BW
- QES provider	n/a for our workstream/scenarios	-	-

4.3 Target country combinations

Relying Party country (Service Provider)	Holder (& authentic source) country (customer)						
		AT	DE	FR	NL	CH	NO
	AT		X		X	X	
	DE	X			X	X	
	FR		X		X	X	
	NL		X			X	
	CH	X	X		X		
	NO	X	X		X	X	

4.4 Requirements

The main requirements for each of the involved roles are included in an Annex.

5 Attestations

5.1 Introduction

This section summarises the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For countries	Requirements
EBWOID	European Business Wallet Owner Identification Data	WP4	DE / AT / CH / FR / NL / NO / IT	
EUCC	European Company Certificate	BU2	DE / AT / CH / FR / NL / NO / IT	
Tax number	Tax number of a legal person (non soletrader)	PA1	DE / AT / CH / FR / NL / NO / IT	
VAT	Tax number of a legal person (non soletrader)	BU3	DE / AT / CH / FR / NL / NO / IT	
Ownership List	Direct owners of the company	PA3	DE / AT / CH / FR / NL / NO / IT	
Control List	Control structure of the company	PA3	DE / AT / CH / FR / NL / NO / IT	
UBO	Ultimate Beneficial Owners	PA3	DE / AT / CH / FR / NL / NO / IT	
IBAN-OV	International Bank Account Number ownership	PA3	DE / AT / CH / FR / NL / NO / IT	

Attestation name	Short description	To be provided by	For countries	Requirements
WUA	Wallet Unit Attestation	WP4	DE / AT / CH / FR / NL / NO / IT	According to EU Business Wallet regulation Article 14/2/b"...Wallet units shall enable authentication and validation of the wallet unit components by presenting the wallet unit attestations..."

5.3 Created attestations in the scenario

Attestation name	Short description	For countries	Applicable domain standards
Social Security Contribution (Note: Social Contribution Clearance might be a better name)	Issued to employers to certify that they have fulfilled their social reporting obligations for their establishments.	FR	unknown
Company Info	Additional company info as a self-declaration, e.g. number of employees.	DE / AT / CH / FR / NL / NO / IT	
DUNS	Data Universal Numbering System number	DE / AT / CH / FR / NL / NO / IT	
LEI	Legal Entity Identifier	DE / AT / CH / FR / NL / NO / IT	
GS1 Global Location Number	Identifier issued by GS1	DE / AT / CH / FR / NL / NO / IT	
Payment Terms	Self-issued attestation defining the payment terms	DE / AT / CH / FR / NL / NO / IT	
Site Attestation	Self-issued attestation for a site of the company	DE / AT / CH / FR / NL / NO / IT	

Attestation name	Short description	For countries	Applicable domain standards
ESG Certificate	Company certificates related Environmental and Social Governance topics (e.g. ISO9000) issued as EAA attestations	DE / AT / CH / FR /NL / NO / IT	

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
User of EUDI Wallet	a.
	b.
	c.
Authentic Sources	a.
	b.
	c.
Relying Party	a.
	b.
	c.
Intermediary	a.
	b.
	c.
EUDI Wallet provider	a.
	b.
	c.
PID provider	a.
	b.
	c.
Trusted list registrar	a.
	b.
	c.
QEAA provider	a.
	b.
	c.
Pub-EAA provider	a.
	b.
	c.
EAA provider	a.
	b.
	c.
QES provider	a.
	b.
	c.

Annex 2 – MVP partner overview

Remark: The following list is a snapshot of the MVP partners as of 2026-06-18. Due to the dynamic nature this might have already become more complete by the day after.

BU1 SC2 (KYS)		Holder (EUBW)					
Attestation type (Issuer)		Bosch (DE)	Bosch (NL)	SBB (CH)	Deutsche Bahn Cargo (DE)	Leone SRL (IT)	Orange FR
EBWOID (LPID)	Business Register QTSP PUBEA	Bundesanzeiger		Bundesanzeiger	Bundesanzeiger		
EUCC	Business Register / BRIS	Bundesanzeiger		Bundesanzeiger	Bundesanzeiger		
Tax NR (company)			Tax administration (NL)				
Tax ID	Central / National Tax Office	Not relevant	Not relevant	Not relevant	Not relevant		
VAT	Self-issued ¹	National Register ²	Tax administration (NL)	Bundesanzeiger	Bundesanzeiger	Infocert?	
ContactPerson	EAA-Attestation	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	
CompanyInfo	EAA-Attestation	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	
GLN	EAA-Attestation ³	GS1 Germany	GS1 Netherlands	GS1 Switzerland	GS1 Germany	GS1 Italy	GS1 France
DUNS (MVP+)							

¹VAT: optionally National Register

²Ministry of finance – currently under discussion with Bundesanzeiger & MoF

³Base GLN is an EAA, derived GLNs are self-issued but tied to the Base GLN

BU1 SC2 (KYS)		Holder (EUBW)					
Attestation type (Issuer)		Bosch (DE)	Bosch (NL)	SBB (CH)	Deutsche Bahn Cargo (DE)	Leone SRL (IT)	Orange FR
LEI (MVP+)		Bundesanzeiger / KVK	Bundesanzeiger / KVK	Bundesanzeiger / KVK	Bundesanzeiger / KVK	Infocert?	
UBO List (MVP+)	EAA-Attestation	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	
UBO List (UBO Register) (MVP+)		Bundesanzeiger	KVK	Not provided ¹	Bundesanzeiger	Infocert?	Notariado
Owner List	EAA-Attestation (QEAA)	Self-issued	Self-issued	Self-issued OR Bundesanzeiger ²	Self-issued OR Bundesanzeiger ⁰	Self-issued	
Control List	EAA-Attestation	Self-issued	Self-issued	Self-issued OR Bundesanzeiger	Self-issued OR Bundesanzeiger	Self-issued	
IBAN	EAA-Attestation	holder (DB; ABN AMRO; Bank ID)	holder (DB; ABN AMRO; Bank ID)	holder (DB; ABN AMRO; Bank ID)	holder (DB; ABN AMRO; Bank ID)		
ESG							
Site Attestation		Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued
Sanction List							

¹CH does not have a Transparency register – bank needs to keep manual process as no registry exists in the country

²Bundesanzeiger to be confirmed

WE BUILD consortium

Specification Scenario 3 & 4 – KYC/KYS for sole traders

WP2 – BU1 KYS/KYC/KYB

Date : 13/05/2026
Version : 1.0 (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)
Status : reviewed (Draft, for review, reviewed, final)

Index

1 Introduction3

- 1.1 *Objectives of this document*3
- 1.2 *Scenario introduction*3

2 Scenario specification4

- 2.1 *Introduction*4
- 2.2 *Scenario pre-conditions*5
- 2.3 *Scenario main flow*5
- 2.4 *Scenario additional flows*6
- 2.5 *Challenges and barriers*6
- 2.6 *Working Assumptions*7

3 Detailed scenario flow8

4 Roles and participants10

- 4.1 *Scenario roles and participants*10
- 4.2 *Additional roles and partners*10
- 4.3 *Target country combinations*11
- 4.4 *Requirements*11

5 Attestations12

- 5.1 *Introduction*12
- 5.2 *Attestations to be provided by other UCs/WGs/scenarios*12
- 5.3 *Created attestations in the scenario*12

Annex 1 – Requirements for scenario roles13

Annex 2 – <name>14

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 3 and 4, as part of use case BU1 KYC/KYS in work package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. During the first months of the project the two scenario's became more the same based on the interactions with our different participants. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important first step towards developing the solutions needed for piloting. Starting with the MVP scenario's and aim for MVP+ later in the project.

1.2 Scenario introduction

Scenario 3: KYC for sole traders

A sole trader (country A) wants to enter into a business relationship with a company in another country (country B) and wants to become a customer. The sole trader initiates the issuance and presentation of required KYC attestations.

Scenario 4: KYS for sole traders

A sole trader (country A) wants to enter into a business relationship with a company in another country (country B) and wants to become a supplier. The sole trader initiates the issuance and presentation of required KYS attestations.

The scenario is based on the following documentation:

- ARF 2.0
- stocktaking document
- WP4: semantic models, issuing PID and EBWOID for sole traders, wallet providers, Deliverable 4.3
- KYC/KYS Directives (such as CSRD2, DORA, AMLR6)
- GDPR & Data Governance Act
- Company Law Directive
- National Business Register law

2 Scenario specification

2.1 Introduction

The two scenarios for sole traders are operated with the same RPs because they are quite similar. Most of the RPs in these scenarios operate in different member states where they want to interact with sole traders. This is interesting from the interoperability perspective. We want to start with member states in which (part of all) sole traders are registered in a business register. In the next phase we want to operate these scenarios in countries where sole traders are registered in a different source (f.i. Tax Agency). In our scenarios we will use the work from PID/EBWOID group Task 4 as input.

Scenario 3

A sole trader (country A) wants to get into a business relationship with a company (country B).

In scenario 3, we take the following perspectives:

1. Know Your Customer (KYC): The sole trader wants to become a customer of the company (country B)

Setting:

The sole trader uses their EBW and/or EUDI wallet (PID) to identify themselves and to present the required KYC related credentials to the company (country B).

2. The following credentials of the sole trader will be processed:

- i. PID
- ii. PoR
- iii. EUCC
- iv. VAT ID
- v. EBWOID from Company B
- vi. TaxID (MVP+)
- vii. EBWOID from the sole trader (MVP+)
- viii. Business license (MVP+)

3. The Company (country B) uses their EU Business Wallet (EBWOID) to identify themselves and to process the KYC related credentials presented from the sole trader.

Scenario 4

A sole trader (country A) wants to get into a business relationship with a company (country B).

In scenario 4, we take the following perspectives:

2.4 Scenario additional flows

Some variations in our scenarios will depend on the availability of registered sole traders in different sources. F.i. in Spain and Italy not all sole traders are registered but this is not blocking for test or pilot purposes in these countries. VAT ID is not yet available in all countries from the start but not blocking for test or pilot. Other variations we think will appear when not all sole traders will get an EBWOID in the beginning but this is also not blocking for test or pilot.

Flow	Short description
Variations	
- Wallet	The scenarios intend to pilot using both EUDIW and EBW wallet or a combination of both wallets.
- EBWOID for sole trader	To be investigated in testing/piloting if PID-data combined with EUCC-data is enough to operate the scenario's or an EBWOID is more desirable.
- Business License	The Gewerbeschein is the official confirmation that a business has been registered with the local trade office in Germany. In an MVP+ scenario we will test a variation with the business license, as it is unique to Germany.
- IBAN	IBAN is part of the MVP+ scenario, because it is not a mandatory requirement in all KYC/KYS flows.
- Certificate of Tax residence	Tax residence is part of the MVP+ scenario, because it is not a mandatory requirement in all KYC/KYS flows.
Exceptions	
-	
- Website	In contrast to the stock taking document, website as an attestation is out of scope. Website is already linked in the EUCC attestation.

2.5 Challenges and barriers

ID	Level	Risk	Measure
1	Low	Delay in finalization or publication of PID / EBWOID protocols in the Implementing Acts and ARF	• Close coordination with WP4 and EC task forces on PID / EBWOID profiles. • Adopt interim semantic mappings and rulebooks from

			EWC / POTENTIAL pilots.
2	Medium	Lack of certified authentic sources, issuers or other roles in front of relying parties/holders	Close coordination with other UC/WP
3	Low	No full geographic coverage of sole traders	Start with the participating countries described in Deliverable 4.3.
4	Low	EBWOID for sole traders	According to the proposal for the regulation on the EBW, sole traders should be able to identify themselves in the EBW via a unique identifier
5	High	Identification of sole traders. Differences in registration process of a sole trader in member states. Credentials will be different.	Make assumptions and select countries based on feasibility of the pilot.

The EUCC Rulebook from EWC depicts a great starting point but needs to be transformed to a shared semantic model that can be reused across use cases. KVK and Infogreffe are both responsible for the EUCC rulebook, which is produced in BU2.

2.6 Working Assumptions

In scenario 3 and 4 we start testing with test data. When progressing towards piloting, learnings will be used to scale the scenarios with the different RPs, sole traders and sources. During pilot phase we will adapt and try to implement real data where possible. The test/pilot strategy is flexible based on presence of RPs in different member states and registration of sole traders in business register or other sources.

Compared to scenario 1 and 2, scenario 3 and 4 will use a smaller set of attestations (for instance, DUNS and LEI are not needed to operate scenario 3 and 4).

In case the scenarios will use the EBW, as provided by the wallet group in WP4 and approved by the WE BUILD testbed, we assume sole traders are able to use these wallets.

Another assumption is that sole traders can receive an EUCC from business registers in the MVP scenario. This is motivated by the argument that multiple business registers in the consortium prefer to issue EUCC to sole traders.

3 Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
1. Download wallet	Sole trader	The sole trader downloads the EUDI Wallet and/or installs the EBW.	Testbed certified wallet implementation must be available.	Two wallet variants supported: EUDIW for same-device flows; EBW for cross-device flows.
2. Generate wallet keys and bind device	Wallet (EUDIW / EBW)	Wallet generates the cryptographic key material required for wallet and attestation binding	Hardware-backed secure storage	
3. Request attestations	Sole trader	User initiates a request through the wallet or issuer interface to obtain the attestations needed for the KYC/KYS process (e.g. PID, EUCC, VAT ID, IBAN attestation).	Wallet keys generated (Step 2). Knowledge of which attestations are required (driven by the relying party's need of attestations in the process).	Required attestation set may differ depending on the the relying party;s KYC/KYS process.
4. Issue attestations	Authentic source & QTSP	Authentic sources (e.g. business register, tax authority) and QTSPs issue the requested attestations to the wallet.	Trusted issuers registered in a Trusted List.	EUCC by business registers (BU2); VAT ID by tax authorities (BU3); IBAN (PA3) only in MVP+.
5. Store attestations	Wallet (EUDIW / EBW)	Wallet stores received attestations for reuse.	Successful issuance (Step 4).	
6. Define KYC/KYS requirements & create QR/presentation request	Relying Party	RP defines the required attribute set (e.g. EUCC, VAT ID, EBWID, IBAN).	RP's KYC/KYS policy (e.g. AMLR).	IBAN, Tax residence and Business license (Gewerbeschein, DE) are MVP+
		RP builds an OpenID4VP presentation request as QR (EUDIW) or copyable URI (EBW).	Defined attribute set.	QR for EUDIW (same-device); URI for EBW (cross-device).
7. Initiate sign-up	Sole trader	Sole trader scans the QR (EUDIW) or copies the URI (EBW) into their wallet.	Presentation request from RP (Step 6); wallet provisioned (Steps 1–5).	Both EUDIW and EBW will be piloted.

8. Process incoming request	Wallet (EUDIW / EBW)	Wallet receives and parses the presentation request.	Valid request from authenticated RP.	
		Wallet displays requested attributes, RP identity and purpose to the user.	Request received and parsed.	
9. Review requested data	Sole trader	User reviews requested attributes, requester identity and purpose.	Request displayed by wallet (Step 8).	
		User consents to sharing the attestations.	Reviewed request.	Refusal ends the flow; selective disclosure may share a subset.
10. Present attestations	Wallet (EUDIW / EBW)	Wallet sends a verifiable presentation of the consented attestations to the RP.	User consent (Step 9); stored attestations (Step 5).	Selective disclosure where supported.
11. Verify & run KYC/KYS checks	Relying Party	RP receives the verifiable presentation.	Wallet sent presentation (Step 10).	
		RP verifies the presentation and trust chain via the EU Trusted List.	Check trusted list; valid signatures.	
		RP runs KYC/KYS checks.	Successful verification.	
		RP evaluates outcome: pass → store; more info → loop to Step 6; fail → reject/manual review.	Completed checks.	Three possibilities: pass / more info / fail.
12. Notify user of outcome	Wallet (EUDIW / EBW)	.Wallet informs the user if the process was successful from the user's and wallet's side.	Outcome from the wallet (Step 10).	

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of EUDI Wallet	Sole trader (consortium members, Google, Deutsche bank, Adyen)	Not restricted, see 3.
2. Authentic sources	KvK	NL
	Infogreffe	FR
	Dutch tax authority	NL
	Registradores	ES
	Infocamere (tbc)	IT
	Bolagsverket	SE
	BRREG	NO
	MRIT	PL
	IRN/ARTE (tbc)	PT
	Skatteverket (tbc)	SE
	Finnish tax administration (tbc)	FI
3. Relying party	Google	HQ in IE, but has multiple offices and customers in member states
	Compliancewise	NL
	Deutsche Bank	HQ in DE, but has multiple offices and customers in member states
	Docaposte	FR
	La poste (tbc)	FR
	Adyen	HQ in NL, but has multiple offices and customers in member states
	Doxallia	FR

4.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
4. Wallet provider	Docaposte	FR	BW
	Digidentity	NL	NW
	iGrant (tbc)	SE	hybrid
	Credenco (tbc)	NL	BW/NW

	SIROS (tbc) Procivis (tbc) Dutch EUDIW wallet	SE AT NL	BW BW/hybrid NW
5. PID Provider	Test data	All participating countries	
6. Trusted list registrar	See below for the QEAA providers		
7. QEAA provider	Docaposte Procivis (tbc) Signicat (tbc) Cleverbase	FR AT NL NL	
8. Pub-EAA provider	KvK Infogreffe Dutch tax agency Bundesanzeiger Bolagsverket BRREG MRIT IRN/Arte (tbc) Skatteverket (tbc) Finnish Tax Agency (tbc) Infocamere (tbc)	NL FR NL DE SE NO PL PT SE FI IT	
9. EAA provider	Not needed for the scenario's		
10. QES provider	Not needed for the scenario's		

4.3 Target country combinations

From an issuance perspective we cover the countries mentioned above and from a verifier perspective we cover all EU member states. As several relying parties, such as Google, Adyen and Deutsche Bank have establishments and customers/end users in multiple EU countries, this makes our scenario's flexible.

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenarios. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Personal identification	WP4 PID EBWOID group	all	In case the sole trader will use an EUDIW only or a hybrid version where a PID is needed
EBWOID	European Business wallet owner identification	WP4 PID EBWOID group	all	In case the sole trader will use an EBW
EUCC	European Company Certificate	BU2	all	Registered in national business register
VAT ID	identifies a taxable person or business	BU3	all	Sole trader needs to be registered at the tax authority
IBAN	International Bank Account Number	PA3	all	Must have a valid IBAN number

As of May 2026, BU3 confirmed real VAT ID can be provided by Finland, Gipuzkoa, Netherlands, Norway. In addition, BU2 confirmed real EUCC can be provided by Netherlands, France, Norway and Sweden.

5.3 Created attestations in the scenario

...

Attestation name	Short description	For Countries	Applicable domain standards
Business License		Germany	Gewerbeanmeldung

We might need to create new attestations depending on the country selected for the sole trader and what unique identifiers they are required to have in that country.

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUDI/EBW Wallet	a. Is a registered sole trader
	b. Registered at a tax authority
	c. Possibly also registered at a business register
2. Authentic sources	a. Able to provide EUCC attestation
	b. Able to provide VAT ID attestation
	c. Assume business registers can issue an EBWVOID
3. Relying party	a. Has a functioning KYC/KYS onboarding platform
	b. Able to onboard a cross-border sole trader
	c. Able to accept PID, EUCC, VAT ID, EBWVOID according Rulebooks
5. EUDI Wallet provider	a. Can hold any of the attestations needed in the scenario
	b. Able to onboard a sole trader to the wallet
	c.
6. PID Provider	a. If PID is not available then it will be a mock attestation or alternative ID-verification-method
7. Trusted list registrar	a.
	b.
	c.
8. QEAA provider	a.
	b.
	c.
9. Pub-EAA provider	a.
	b.
	c.
10. EAA provider	a.
	b.
	c.
11. QES provider	a.
	b.
	c.

Annex 2 – <name>

...

WE BUILD consortium

Specification Scenario 5 – Know Your Employee

WP2 – BU1

Date : 19.06.26
Version : 1.0 (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)
Status : Final (Draft, for review, reviewed, final)

Index

1	Introduction.....	3
1.1	<i>Objectives of this document</i>	<i>3</i>
1.2	<i>Scenario introduction</i>	<i>3</i>
2	Scenario specifications	5
2.1	<i>Introduction</i>	<i>5</i>
2.2	<i>Scenario pre-conditions</i>	<i>7</i>
2.3	<i>Scenario main flow</i>	<i>9</i>
2.3.1	<i>Employee credentials</i>	<i>9</i>
2.3.2	<i>PD A1</i>	<i>10</i>
2.3.3	<i>Posted Worker Notification (PWN) (Netherlands)</i>	<i>19</i>
2.4	<i>Additional flows.....</i>	<i>22</i>
2.5	<i>Challenges and barriers.....</i>	<i>23</i>
2.6	<i>Working Assumptions.....</i>	<i>23</i>
3	Roles and participants.....	24
3.1	<i>Scenario roles and participants</i>	<i>24</i>
3.2	<i>Additional roles and partners</i>	<i>24</i>
3.3	<i>Target country combinations</i>	<i>25</i>
3.4	<i>Requirements</i>	<i>25</i>
4	Attestations	26
4.1	<i>Introduction</i>	<i>26</i>
4.2	<i>Attestations to be provided by other UCs/WGs/scenarios</i>	<i>26</i>
4.3	<i>Created attestations in the scenario</i>	<i>26</i>

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 5 '**Know Your Employee (KYE)**', as part of use case BU1 in work package 2 of WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The document is the result of the Specification Phase of the WE BUILD Large Scale Pilot and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

The KYE scenario can basically be summarised as following:

An employee from company A in country A has to deliver a service in a company B in country B.

This use-case, which applies millions of times annually within Europe, is essential to facilitate the one single market vision from the European Commission. Mainly three credentials will specifically be tested in this scenario:

1. Employee VC is a proposition
2. A1 is following EU regulation
3. PWN attributes and process flow has been validated by the Dutch Ministry of Social Affairs and Employment, Spanish labor inspectorate and Finnish Centre for Pensions.

The pilot would be composed by two phases:

Phase1 Synthetic data

- Member State wallets do not let issuance of credentials. Therefore, private wallets will be used
- Real PID issuance is not yet ready which would also not allow the use of real data.
- Therefore, the objective is to demonstrate UX and flows and become as close as possible to a 'market ready' state (how EUDI wallet simplifies the current situation)
- Demonstrate cross-border interoperability

Phase2 real data

- Requires the signature of Data Protection Agreements between stakeholders
- PID, EBWID, EUCC and memberstate Wallets need to be ready

The scenario is based – among others - on the following documentation:

- Directive 2006/123/EC
- Regulation (EC) No. 883/2004 on the coordination of social security systems (especially Articles 11-16)
- Regulation (EC) No 987/2009 implementing Regulation (EC) No 883/2004 on the coordination of social security systems [Regulation - 987/2009 - EN - EUR-Lex](#)
- Directive - 2014/67 - EN – EUR-Lex

- Directive 96/71/EC of the European Parliament and of the Council of 16 December 1996 concerning the posting of workers in the framework of the provision of services (as amended by Directive (EU) 2018/957) EUR-Lex - 01996L0071-20200730 - EN - EUR-Lex
- COMMISSION IMPLEMENTING REGULATION (EU) 2024/2977 of 28 November 2024
- ARF v2.8.0

2 Scenario specifications

2.1 Introduction

The Services Directive ([Directive 2006/123/EC](#)) strengthens the freedom to provide services within the EU. This directive is crucial for the completion of the internal market, since it has huge potential for delivering benefits to consumers and SMEs. The aim is to create an open single market in services within the EU, while at the same time ensuring the quality of services provided to consumers. According to the [Commission communication entitled 'Europe 2020 – A strategy for smart, sustainable and inclusive growth'](#), the full implementation of the Services Directive could increase trade in commercial services by 45% and foreign direct investment by 25%, bringing an increase of between 0.5% and 1.5% in GDP. The directive contributes to administrative and regulatory simplification and modernisation.¹

It is important to note that the European Commission has set ambitious goals for 2024-2029 and beyond. These goals are designed to boost Europe's competitiveness by creating a faster, simpler, and more united Union. This starts with making business easier and faster across all sectors and tackling the skills and labour gap. Europe's Single Market should allow services and people to move freely and opening up markets. The focus will be on reducing administrative burdens and simplifying implementation: less red tape and reporting, more trust, better enforcement, faster permitting. They will also address the patchwork of national regulations that makes doing business in different EU countries more complicated.

Hence, the main objectives of this scenario are:

- 1) demonstrate the positive impacts and the benefits of the European wallet ecosystem to simplify complex administrative processes
- 2) test the usability of personal data exchange
- 3) demonstrate cross-border and cross-jurisdiction data exchange

Scenario5 Know Your Employee (KYE) is part of BU1 and will lead to MVP and MVP+ implementations. It will use both Natural Person Wallets and Legal Person Wallets. The high-level scenario description is the following:

"A company A in a country A would like to send one of their employees to work and provide a service to company B in country B."

This scenario requires essentially the issuance of three main credentials:

1. Employee Credential
2. Portable Document A1 (PD A1, also "A1 certificate")
3. Posted Worker Notification (PWN)

¹[Freedom of establishment and freedom to provide services | Fact Sheets on the European Union | European Parliament](#)

Employee Credential: Credential issued by an employer to all its employees to certify that they are part of the company. The only quality given to the employees by this credential is to certify that they work for that company in a given point in time. Additional qualities could be provided by other credentials such as Power of Attorney (PoA) or Signatory Rights (SR) to sign contracts or transactions.

The applications of such a credential are numerous. It could be helpful in certain transactions of goods (eg truck drivers), to access company assets, to download certain credentials linked with labor regulations (eg PD A1, PWN), to access to certain benefits (eg rebates,...) etc.

PD A1: The Portable Document (PD) A1 is a certificate that documents the applicable legislation regarding social security in a cross-border employment situation. The PD A1 is uniformly regulated for members states of EU, EFTA, and the United Kingdom. The main legal basis is Regulation (EC) No. 883/2004 on the coordination of social security systems (especially Articles 11-16). By granting several exceptions to the principal rule – that a person is subject to the legislation of the member state where the work is pursued –, it supports mobility for working citizens while protecting their rights. In the here relevant “classic” posting situation – where a citizen works abroad for a maximum of 24 months –, the social security institution of the “sending” state issues a PD A1 which states that the legislation of this “sending” state stays applicable throughout the temporary posting (to ensure continuous coverage and to avoid e.g. dual contributions). (Further legal aspects can be found in Regulation (EC) 987/2009 and in national legislation regarding social security.) In the most current reporting period (2024), 5.6 million PDs A1 were issued.² The PD A1 use case holds massive potential for more efficient processes for all involved actors. Due to its importance for the free mobility of workers while ensuring their social security rights, the PD A1 is one of the main use cases of the “European Social Security Pass” initiative of the European Commission. The work done here regarding the PD A1 can be seen as a complementary action with a specific WE BUILD focus. An alignment with the ESSPASS initiative is welcome – this scenario implementation could explore specific approaches that are discussed within ESSPASS and also contribute to the ESSPASS discussions.

Attestation Rulebook for attestations of type Portable Document A1 (PD A1)

<https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/blob/main/rulebooks/rb-a1/README.md>

PWN: Posted Worker Notification (PWN) is an administrative requirement for companies (legal employers) that provide intra-EU cross-border services with their employees, both EU and non-EU nationals, either to a customer or into another group entity. The notification was introduced pursuant to an EU Directive³⁴ [Directive - 2014/67 - EN – EUR-Lex](#) and needs to be filed with the authorities of the host EU Member State (usually on a government portal) prior to the start of the delivery of the service. The PWN was introduced to enable EU

²Source: European Commission: Directorate-General for Employment, Social Affairs and Inclusion, De Wispelaere, F., De Smedt, L. and Pacolet, J., Posting of workers – Report on A1 portable documents issued in 2024, Publications Office of the European Union, 2026, <https://data.europa.eu/doi/10.2767/4941289>, page 10.

³<https://eur-lex.europa.eu/eli/dir/2014/67/oj/eng>

⁴[EUR-Lex - 01996L0071-20200730 - EN - EUR-Lex](#)

Member States to monitor that Posted Workers are protected by the salary and labour conditions set out in host legislation and collective labour agreements and therefore do not undercut local labour force. More or less half of the EU member states have extended the scope of the PWN also to employers based outside the EU. The labour law protection of posted workers is set out in the Posting of Workers Directive (PWD) which was adopted in 1996 and revised in 2018. [EUR-Lex - 01996L0071-20200730 - EN – EUR-Lex](#)

Attestation Rulebook for attestations of type Posted Worker Notification (PWN)
<https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/blob/main/rulebooks/rb-pwn/README.md>

2.2 Scenario pre-conditions

One of the most important pre-conditions is to have wallets that allow the issuance of credentials (eg employee credentials, PD A1, PWN). Currently, most of the Member States are restricting that possibility in their state-operated wallet versions. This is a major limitation and requires in our case the use of multiple wallets (eg state-operated ones containing the PID, private ones receiving credentials). This configuration is obviously sub-optimal in terms of user-experience. In certain circumstances, it might even not be possible to implement the use-case if the issuer of a credential requires to issue his/her credential in the same wallet that the one presenting the PID (eg for authentication reasons).

PID, EBW/OID credentials should be issued by the relevant authorities according to the associated rulebooks available on WEBuild consortium github:

- [webuild-attestation-rulebooks-catalog/rulebooks/ds001-ebw-oid-rulebook.md](#) at main · [webuild-consortium/webuild-attestation-rulebooks-catalog](#) · GitHub
- [webuild-attestation-rulebooks-catalog/rulebooks/ds002-pid-rulebook.md](#) at main · [webuild-consortium/webuild-attestation-rulebooks-catalog](#) · GitHub

The PD A1 process itself, especially the “classic posting situation” is a European-wide regulated, mostly generic use case. Nevertheless, to be able to grant an effective “real world” pilot design involving the central issuing institution in WE BUILD, Deutsche Rentenversicherung Bund (DRV Bund), the following pre-conditions have to be met:

- While special cases like multi/cross-border employment, postings exceeding 24 months per the exception agreement, self-employed persons, etc. can be also relevant for PD A1 issuance, in our scenario, an employee of Company A in country A is sent to work for company B in country B for max. 24 months.
- Based on the German legislation with “split responsibilities”, the PD A1 can only be issued by a DRV (German Pension Insurance) institution if the posted worker has a private health insurance (and is by consequence not covered by the statutory health insurance). The posted worker additionally must not have a specific “professional” coverage.

The BU1 Sc5 scenario is, as other scenarios, based on general requirements regarding a Trust Framework on which the wallet ecosystem operates. These should, for piloting purposes, be

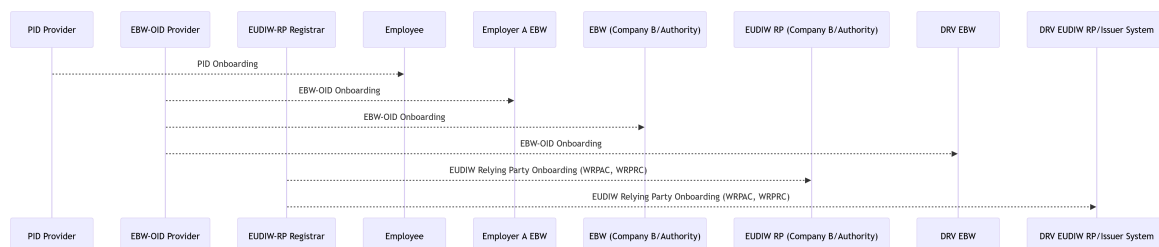
aligned and coordinated (especially within WP4) for the whole WE BUILD consortium while some use case/scenario specifics might come into play. A non-exhaustive and more high-level list of such requirements, with a partially special focus on the PD A1 use case and a real-world uptake, can be formulated as follows:

- Attestation Issuers must be onboarded and verifiable.
- Where relevant, a secure connection from Authentic Sources to Issuers must be established.
- Issuers must be accredited to issue PD A1 (analogue to EESSI Institution Repository, also cross-sectoral accreditation possible). This accreditation must be verifiable.
- Issuers should be accredited to request and process a PID (or parts of it + maybe other identification means). This accreditation should be verifiable.
- A schema for PD A1 as (Q/PuB-)EAA must be defined and registered. The schema must be publicly accessible for validation.
- Attestation Issuers as a whole institution as well as specific accreditations must be revocable.
- The Attestation Issuer must be able to verify the authenticity of the citizen's EUDI Wallet Instance and also be able to verify the presented credential (necessary: Wallet Issuer List, wallet Instance (revocation) list, PID issuer list, PID instance (revocation) list, ...). This applies also for European Business Wallets and their Owner Identification Data.
- The Attestation Issuer must be able to unambiguously identify the EUDI wallet user based on the presented identification data (additional data to PID, e.g. other attestations, might be necessary). This applies also for European Business Wallets and their Owner Identification Data.
- The PD A1 as a Verifiable Credential (Q-EAA/PuB-EAA/EAA) should only be issued to the rightful owner (by identity matching procedures). The PD A1 may also be issued to other authorised persons (e.g. an employer representative).
- The issued Attestations must be revocable by the issuer (only). This attestation revocation information must be publicly available for the verification process.
- To prevent traceability and to grant performance, such an attestation revocation list should not be managed by every issuer separately, but be managed on a "more central" position, e.g. on national and/or sectoral level.
- Authorised Verifiers (Wallet Relying Parties) should be onboarded and verifiable.
- If relevant, Verifiers should be accredited to request PD A1 and PID (or specific subsets of these attestations). This accreditation should be based on policies and should be publicly available.
- Regarding representatives of a "verifying institution", there should be clear and verifiable onboarding and role-based access mechanisms.
- The citizen must be able to verify that he/she faces a legitimate representative of an accredited institution and that this specific representative has the accreditation to perform the intended action.
- In the process of "mutual authentication" between citizen and verifier representative, also the representative's personal data must be protected (while disclosing enough data to grant a relevant transaction logging for specific purposes).

- There should be a central or national “attribute verification policy register” which should be consulted in the verification process; the results should be displayed to the citizens (and beforehand, at request preparation, to the verifier).
- For the verifier, it should be possible to prove the legitimate possession of a presented attestation, e.g. by validating if the wallet instance which presents it is the same one that it was issued to. Nevertheless, the verification process must also allow flexible elements and therefore must not only rely on strict bindings – e.g. if the content was migrated to a different wallet (instance), the EUDI wallet contains no valid PID (or the citizen does not want to use it), attestations have been rightfully transferred (e.g. delegated to a representative), etc.
- The trust framework should allow offline verification (eg for on-fields audits).

Onboarding of actors:

The relevant actors of the scenario must be onboarded by attestation providers or registrars. As an example, for the PD A1 flow (DRV = attestation issuer), the onboarding steps must contain the following steps:



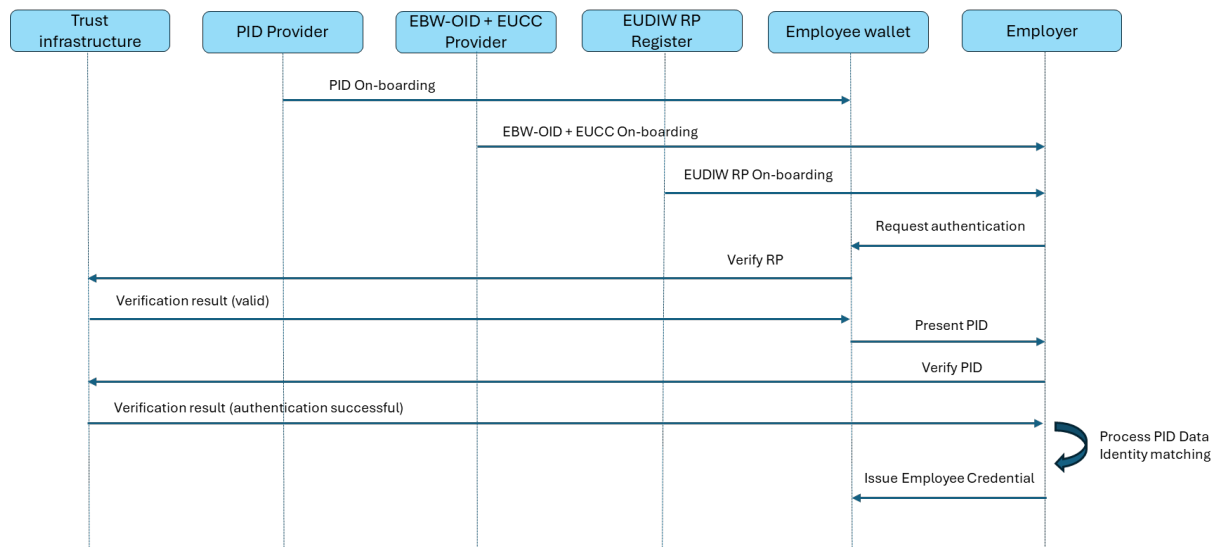
2.3 Scenario main flow

2.3.1 Employee credentials

The main objective of an employee credential is simply to prove that a person is effectively working for a given company. Therefore, the employer has to put in place an identity verification process (online or face to face), usually complementing the usual employee onboarding process. As a result of this identity verification (using the PID), the employee should receive his/her employee credential containing notably the name and identifier of the employer and personal data from the employee (name, surname). We suggest also the employer to define an identifier, called badge number, different from the employee number. The reason is that this badge number could reference uniquely the employee in various use-cases while keeping company employee private data safe.

Attribute name	Short description	Optionality
Name	Employee name	Mandatory
Surname	Employee surname	Mandatory
Credential identifier	Badge number	Mandatory Company identifier (Machine readable) - Union Database for

		Biofuels Info-site - EC Public Wiki
EU company ID	EU company ID	Mandatory
EU company name	EU company name	Mandatory



Rulebook on Employee Credential on GitHub:

[webuild-attestations/rulebooks/rb-employee/README.md](https://github.com/flo0x/webuild-attestations/blob/main/rulebooks/rb-employee/README.md) at main · flo0x/webuild-attestations

2.3.2 PD A1

As stated above, to grant an efficient pilot design, the PD A1 use case as described below is based on the national/institutional flow where a PD A1 is issued from the German institution “Deutsche Rentenversicherung” (DRV). While the process itself is generic in most of its aspects (as European social security coordination rules apply), minor national specifics may exist.

2.3.2.1 PD A1 request and issuance

The PD A1 use case in our classic posting situation is always triggered by the employer. To apply for a PD A1 for its posted worker, this employer has to send a corresponding request/application to the responsible national institution.

2.3.2.1.1 Status Quo (Current process)

Application and issuance:

Currently, the request/application is sent by the employer – as legally foreseen in Germany – mandatory in a defined XML format via the employer’s payroll/accounting system or via the manual usage of a common portal (“SV-Meldeportal”). If the pre-conditions are met (see

above), following specific national routing rules, the electronic request/application by the German employer reaches the “employer-communication endpoint” of Deutsche Rentenversicherung (DRV). To communicate with this endpoint, the employer has to use a specific employer certificate.

Please note that this part of the process might have important country specifics (regarding split or central responsibilities, ways of submission for a PD A1 application etc.).

In our specific case, DRV now receives the request and checks it (e.g. for overall legitimacy, illegal chain of postings etc. – also regarding responsibility of the single institutions). It has to be mentioned that the DRV (Deutsche Rentenversicherung) consists of 16 institutions (i.e. 16 authentic sources). The PD A1 is currently issued by one of these institutions based on internal routing/competence rules. Nevertheless, only one of the 16, DRV Bund, provides the common service point for the interactions with employers in the PD A1 use case.

If the request is approved, the employer receives – over the same communication channel as for the application - an “approval” in XML format with the corresponding PD A1 in PDF format attached.

(Additionally, DRV sends a “posting notification” via the “EESSI” (Electronic Exchange of Social Security Information) system to the competent institution abroad, where this information can be provided to national verifying authorities).

The employer then processes the XML, stores the A1 PDF in their personal registers and forwards the PDF (or a printed paper version) to the employee. Both the employer and the employee have the A1 on file in case of queries or an inspection by the relevant authorities in the host country where the services are performed.

Role of employers:

Employers in the sending State:

The employer in the sending state has a central responsibility in the A1 procedure. In the case of a cross-border activity, the employer shall apply for the A1 certificate for the employed person to the competent social security institution of the sending State ‘in advance, whenever possible’. The employer shall immediately provide the employee with the A1 certificate, as a PDF document by e-mail or printed out as a paper certificate.

Contracting entities in the State of employment:

Experience has shown that, in practice, contractors in the State of employment require a copy of the A1 certificate even before carrying out the activity in the State of employment (e.g. when working on a construction site). Therefore, the A1 certificate is currently often provided by the employer in the sending State to the contracting authority in the State of employment by e-mail. A copy of the A1 certificate shall be submitted to the contracting authority as a paper certificate by the person posted at the latest.

Experience has shown that the contractor needs a copy of the A1 certificate for various reasons:

On the one hand, the A1 certificate serves as proof for the contracting authority in the State of employment that it does not have to pay social security contributions for the duration of its activity in the State of employment. The applicable law documented in the A1 certificate – in this case German social security law – is binding on the Member States concerned as long as the A1 certificate has not been revoked.

In addition, many Member States, such as France, Austria, the Netherlands and Switzerland, have strict labour/customs or social security checks based on national legislation. The A1 certificate must be presented during such checks by the employer in order to avoid fines and other penalties.

In practice, the A1 certificate is also an important document for the contracting authority in the State of employment.

2.3.2.1.2 To-be process

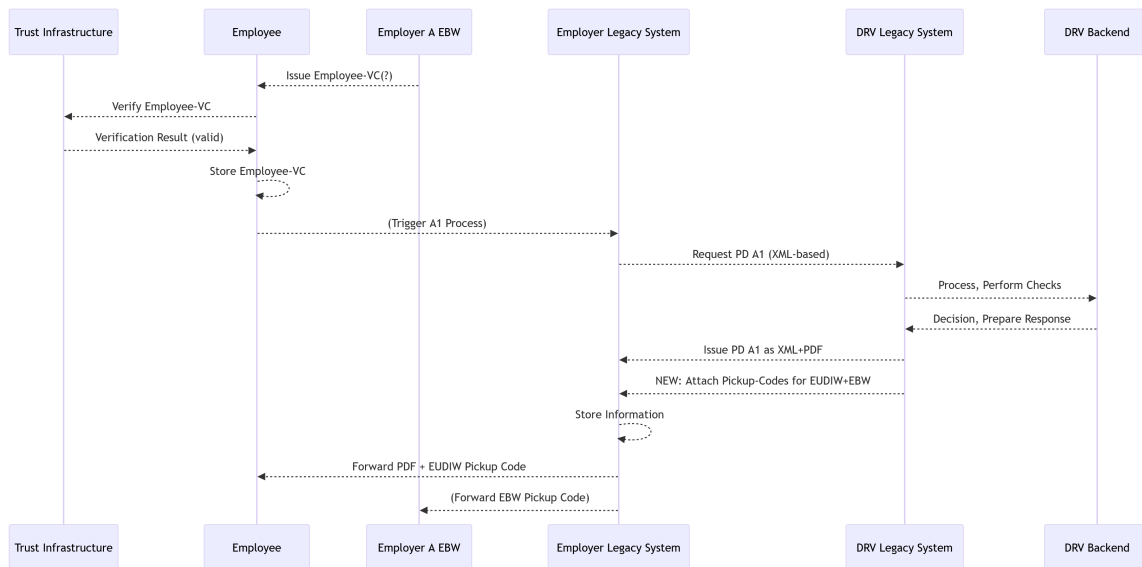
To grant a more efficient process, the scenario should be defined as follows:

The request still has to be sent from the employer to the competent institution. A new process including the usage of the European Business Wallet (EBW) to submit the request (“triggering process”) currently might bring no significant benefits for the involved actors in our specific “German” setting. Therefore, the well-established existing request process (“triggering process”, see above) should persist: in the defined XML format via the employer’s system or via the manual usage of a common portal to DRV’s dedicated endpoint. For other countries where such an efficient status quo application process might not exist (and instead higher administrative burden), the usage of a European Business Wallet for the application process might be worth exploring.

To get benefits for the involved actors, in general as for the German piloting use case, there should be a NEW modified response from the issuing institution to the requesting employer after the request has been approved: Additionally to the existing content, this response should contain one or more download links/“credential offers” to receive the PD A1 also as a Verifiable Credential. The purposes are:

a) to be forwarded to the posted person to download the PD A1 directly from DRV’s issuing system to his/her **personal EUDI Wallet**.

b) to be used to download the PD A1 as a credential directly from DRV’s issuing system to the **employers European Business Wallet** for document-retention purposes in the personnel register and for potential inspection services by relevant host country authorities.



In the following steps, please note that DRV Bund will also issue VCs “on behalf” of all 16 German Pension (DRV) Institutions. Further details regarding this constellation (e.g. for onboarding) have to be analysed later.

Further process for (a):

The posted employee follows the download link and gets a credential offer for his/her EUDI Wallet (containing the issuer’s URL, document number etc.).

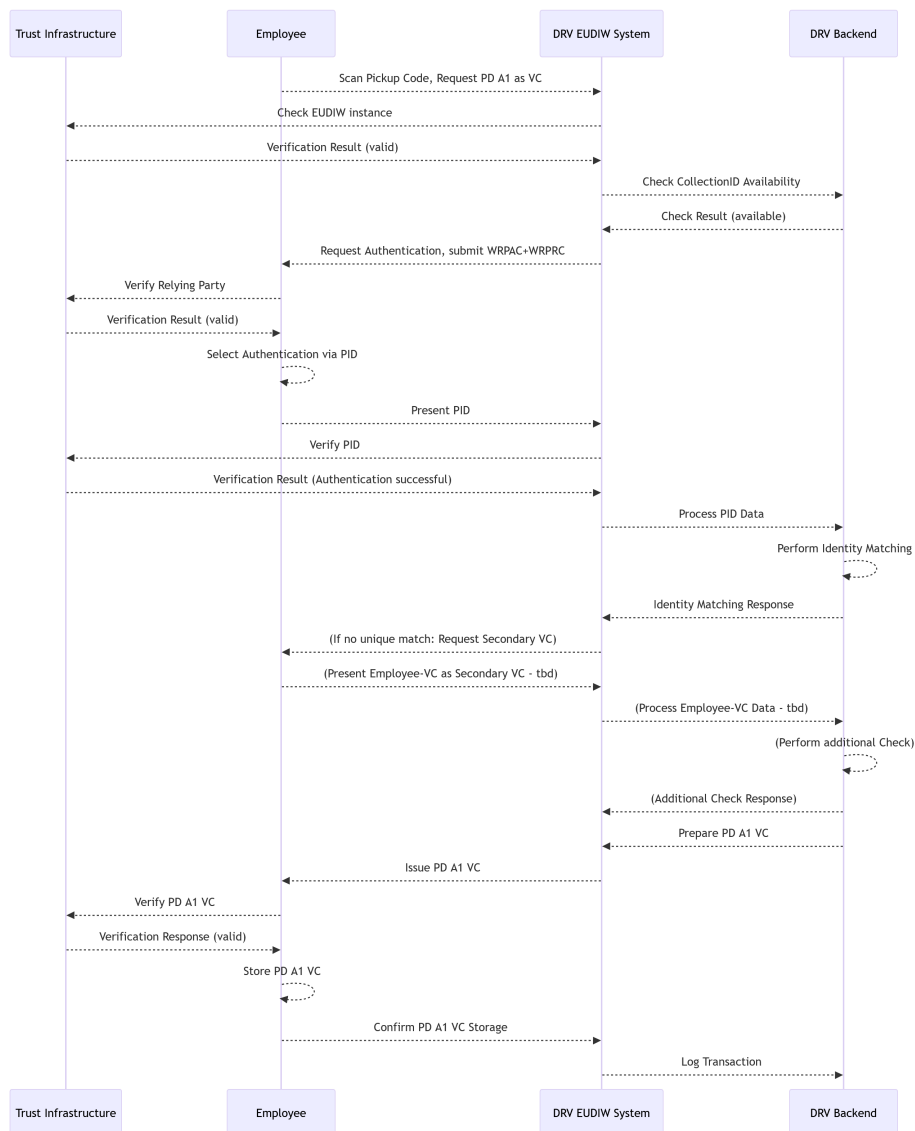
Before the PD A1 can be issued, DRV’s issuer system has to perform **basic checks** regarding the EUDI Wallet (see preconditions). The EUDI wallet also performs basic checks if DRV Bund is entitled to request a PID and to issue a PD A1 (see preconditions).

DRV Bund then also has to perform an **identity check** as they have to grant that the PD A1 is only issued to the rightful owner. For this, DRV Bund asks the citizen for authentication (via PID, maybe also different methods). As the German PID does not contain a unique identifier and PIDs from other countries might not be “matchable”, DRV Bund has to perform a (semantic) **identity matching** procedure. For this, additional data from the citizen might be necessary to grant the necessary assurance.

In the context of the “identity matching challenge”, it has to be mentioned that specific approaches for granting a secure identification without unique identifiers are currently discussed. An important approach is the usage of additional “secondary credentials”(like the German tax number, a social security number etc.). While WE BUILD might decide to avoid this central topic, it is clear that this challenge exists, has a big impact on the whole ecosystem and should be tackled. Even if the “business aspects” of this challenge are left to other actors outside WE BUILD, at least the “technical” part of a secondary credential could be explored within WE BUILD. Here, the employee VC might come into play. While it does not grant 100 % identification security (or solve the problem itself), this VC could be used to grant a “higher” security in Person Identification (as it serves to know that person X has not only a fitting PID, but also works for the applying employer). More relevant, this VC could be used to explore/pilot the usage of the “Interactive Authorisation Endpoint” which is foreseen

for OpenID4VCI version 1.1 – in that sense, the employee VC could be requested and presented only (as a second authentication step) if the personal data is not sufficient for a unique identification.

In any case, if the identity check/matching is successful, the PD A1 is issued as a VC (EAA) to the EUDI Wallet. For this, the VC has to be created according to the defined schema, has to be signed and sealed etc. Please note that there might be specific “binding options” which affect the usage flexibility (more aspects regarding this see below).



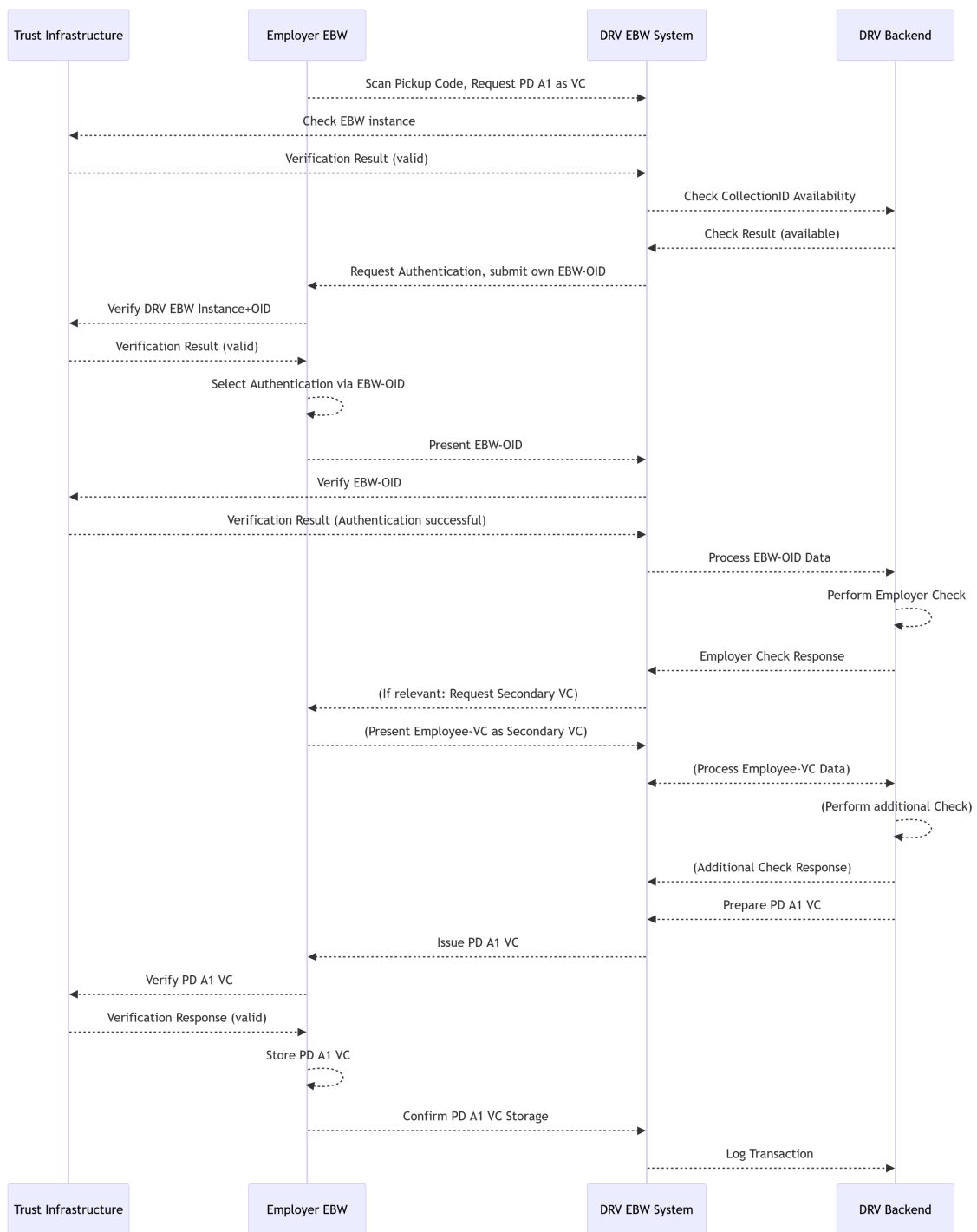
Further process for (b):

The entitled user of the employer’s EBW (e.g. an HR employee) follows the provided download link/credential offer (containing the issuer’s URL, document number etc.) using his/her European Business Wallet Unit.

Before the PD A1 can be issued, DRV's issuer system has to perform basic checks regarding the EBW unit (see preconditions). The EBW unit also checks if DRV is entitled to request a PID and to issue a PD A1 (see preconditions).

Parallel to the "identity check" for the employee, DRV then also has to perform an "eligibility check" for the employer – as personal data is affected and DRV has to grant that the PD A1 is only issued to a rightful user of the requesting employer. For this, the EBW user has to share the EBW Owner Identification Data (OID) and DRV has to check if this matches to the requesting employer's certificate.

If the "eligibility check" is successful, the PD A1 is issued as a VC (EAA) to the European Business Wallet. For this, the VC has to be created according to the defined schema, has to be signed and sealed, etc.



General comment:

It has to be mentioned that ongoing discussion also cover the usage of Verifiable Credentials/Electronic Attestations of Attributes outside a wallet (e.g. QR code based, PDF with “embedded credential” etc.) or in wallets without an identity. This has a big impact on the flexibility of the usage of an attestation like the PD A1. WE BUILD might want to explore specific settings in this context based on current discussions in other initiatives.

2.3.2.2 PD A1 Verification

The posted worker now works for company B abroad (e.g. in the Netherlands). In the verification/usage scenarios abroad lies maybe the most potential for an increase of efficiency within the PD A1 use case.

The possible scenarios can be grouped as follows:

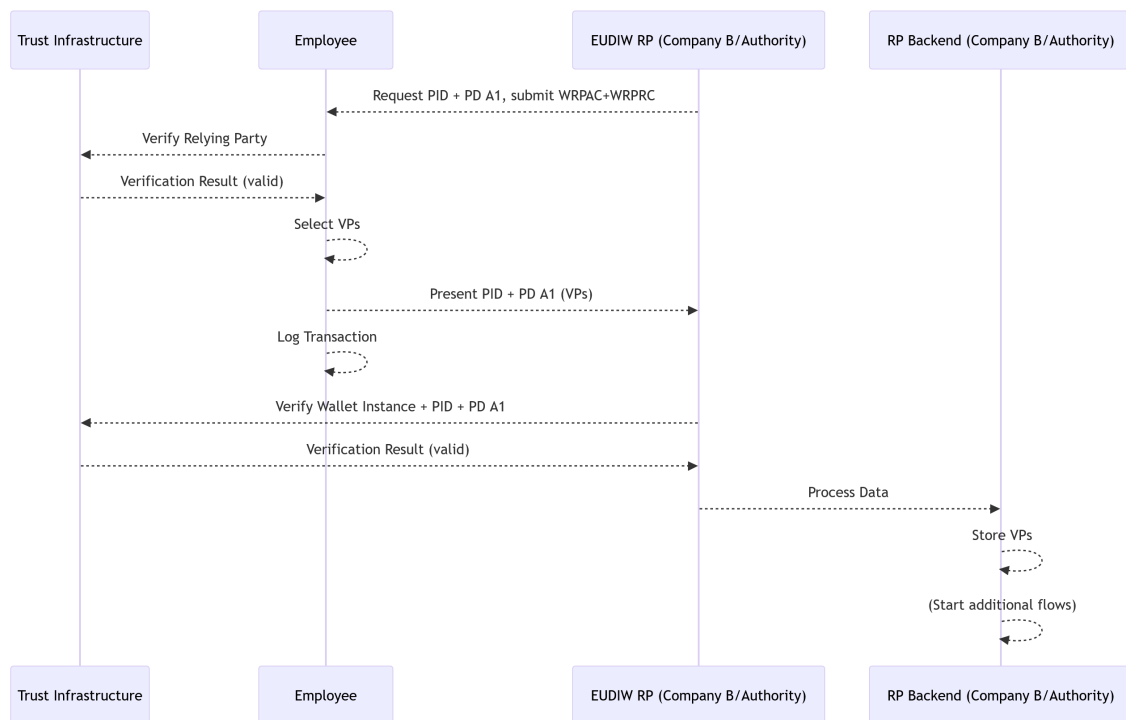
a) Verification of the citizen's credentials by an official authority

While the citizen is working, a representative of the relevant Dutch authority (customs, financial police, labour and social security authority, inspection services, etc. - "Verifier") visits the company site and wants to perform a verification.

Status quo process: The Verifier asks the posted worker for his/her PD A1 and an identity document. He/She receives it in paper/card format. First, the verifier checks if the identity data on the PD A1 matches the presented identity card. He/She then verifies the identity card itself. To check, if the PD A1 is not forged, he/she has to check if there is a corresponding posting notification in the system. For this, he/she checks a national database to see if the competent institution from the sending state submitted such a notification via the EESSI system. If all is okay, the verifier creates a record. All in all, this describes the current time-consuming process.

To-be process: The Verifier asks the posted worker for his/her PD A1 and an identity evidence using an EUDI compliant Verifier App (maybe new: Business Wallet Unit). The onboarded verifier creates a request for Verifiable Presentations of a PD A1 and the PID (or subsets of these; the role of the PID in the verification process may be discussed). The Verifier's mobile device displays a QR code (and optionally a picture of the Verifier). The posted worker compares the Verifier's face with the picture (if applicable), then scans the QR code (directly out of EUDI wallet or EUDI Wallet opens now) and receives the Verifier's request. He/She automatically checks if the Verifier App (maybe EBW unit) is valid and if the Verifier is authorised to ask for the requested information. The posted person also sees (and logs) basic information about the verifier, e.g. a service number. The EUDI wallet displays all this and also the information that has been requested to present.

The EUDI wallet then proposes fitting VCs to the user and offers Selective Disclosure options. The worker confirms the right VCs and agrees to submit them (a subset or as a whole) to the Verifier. The Verifier's device receives the VPs remotely and performs the relevant checks (valid wallet, PDA1+PID not revoked, from an authorised issuer etc.). The result is displayed to the Verifier. He/she can now process the data to his/her back-end with just clicking a button. The worker receives a notification that the submission was successful (further steps, e.g. report about the results to be defined as depending on the connection). All in all, this can happen in a very short time and therefore describes the new efficient process.

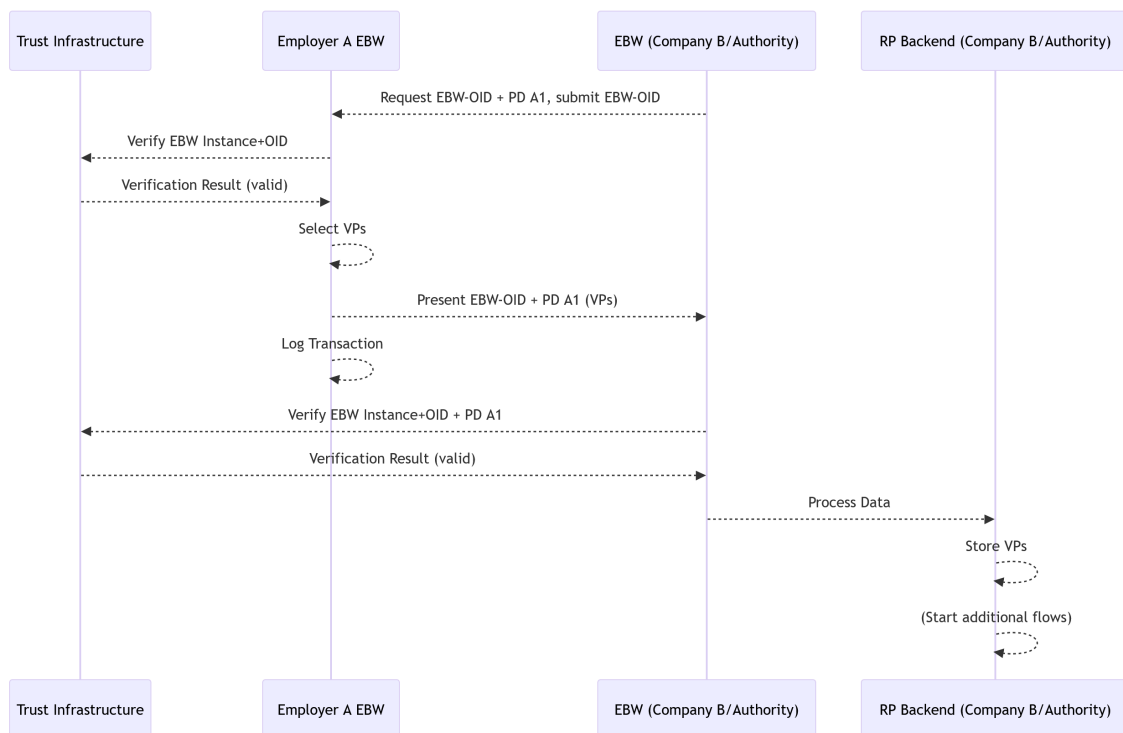


b) Verification of the citizen's credentials by the employer/contractor abroad

While/before the citizen is working abroad, a representative of the employer/contractor in the “receiving state” might also want to verify if the posted worker meets the formal requirements (e.g. for due diligence purposes). The process mainly matches the verification scenario (a) above – with the difference, that the verifier is not a representative of an official authority but of an employer/contractor. This representative can also use a Wallet Relying Party system or an EBW unit to verify the PD A1 (and identity data). For data protection purposes, specific rules (e.g. only minimal data) might apply.

c) Verification of the employer's credentials by Relying Party “company B abroad”

For business/due diligence purposes, also company A may want to present a PD A1 (+maybe other credentials) to company B (as a Relying Party). This EBW-EBW-communication would have to be worked out based on the Business Wallet specifications (respectively the WE BUILD interpretations/assumptions). If this process mainly matches scenario (a), it can be illustrated as follows:



d) Verification of the employer's credentials by Relying Party "Official authority abroad"

For business/due diligence purposes, an official authority (e.g. customs, financial police) may request the presentation of a PD A1 (+maybe other credentials) from company A. This EBW-EBW-communication would have to be worked out based on Business Wallet specifications.

e) Verification of already "presented" credentials by another Relying Party

In practice, company B might also be asked by the local authorities to share PD A1 (+maybe other credentials) which were issued to company A and only presented to/as a "copy" received by company B. It has to be defined how this process could look like (e.g. copy of the VC or copy of the VP or other methods).

f) General comment: We favor/want to explore an approach with a very "flexible" handling of the PD A1 VC. As the PD A1 is anyway not only issued to the corresponding citizen, but also to the employer, the VC has to contain the data of the VC subject in any case. The business flow for the usage is also in practice mainly that the employee or employer from the "sending state" have to share the PD A1 VC with an employer/contractor abroad. In a second step, this employer/contractor abroad is e.g. checked and has to share the PD A1 VC with a national authority. Therefore, a solution where there is no strict holder binding but - on the opposite - only a "loose" or optional binding which allows it to "copy" the PD A1 VC, is favored. This would grant that the receiving entity can share it again with another relevant entity. It could be worth to explore within WE BUILD how such a solution could look like (especially from a technical point of view).

2.3.3 Posted Worker Notification (PWN) (Netherlands)

Another example of an important administrative burden for companies doing business throughout the EU is the **Posted Worker Notification (PWN)**.

Unlike a PD A1, the Posted Worker Notification does not have an approval process but is rather a notification to the host EU Member State Authorities. The application process, data fields, such as PII (e.g. First name, Last name, data birth, national security ID, etc...) and documents required for the lodging of the Posted Worker Notification vary by Member State. The non-compliance is a major pain point for the European Labour Authority (ELA), the EU institutions and the Member States.

In addition, the application process varies across EU Member States with some Member States even requiring a signature on the PWN application (e.g. wet, digital or qualified signatures, etc...).

The European Commission has proposed a Regulation on a public interface connected to the Internal Market Information System for the declaration of posting of workers and amending Regulation (EU) N° 1024/2012 ([Proposal on a public interface for declaring posted workers - Internal Market, Industry, Entrepreneurship and SMEs](#)) aiming at simplifying and standardising the PWN, thereby reducing administrative burden and improving compliance and enforcement across Member States. The draft Regulation references the European Digital Identity Framework for the facilitation of the identification and potentially the issuance of the PWN. Means in which applicable information relating to Posted Workers is gathered, verified and shared is evolving quickly and the Digital Wallet will become critical for ensuring that companies doing business in Europe can be compliant while taking full advantage of the single Internal market.

2.3.3.1 Scenario pre-conditions

A **Company** wallet could be expected to have verifiable credentials (VC) for the following:

1. Power of Attorney (PoA) VCs – PoA might be needed to sign documents, to create accounts and file on government portals, to engage a service provider, etc.
2. Business Wallet for supply of services will need to include registration of the business register, VAT number, attestation of compliance with home-country and host-country employment and tax requirements, service agreement, list of employees engaged in the project and their PD A1/PWN, general and sector-specific authorizations/notifications.

An **Individual** wallet could be expected to have verifiable credentials (VC) as following:

1. PID VC
2. Work and residency certificates for the home-country VC
3. Visa/work authorization for the Host-Country VC
4. PD A1/PWN VC
5. European health insurance card VC

6. VCs for all the employment-related documents that one needs to keep on file such as employment contract and assignment letter, payslips, time sheets etc.

2.3.3.2 Scenario main flow

A company in country A (Germany) has a contract to supply specific cross border services to a client in country B (Netherlands). The contract requires an employee of the German company to travel to the Netherlands for a few weeks to conduct consulting services. The employee that has been selected is a German national living and working in Germany. The German employer company has to file a Posted Worker Notification with the Dutch authorities, specifying the details of the Posted Worker, the employing entity in Germany, the client in Netherlands, as well as details surrounding the actual work location.

The Dutch Posted Worker Notification will require specific information identified below. The attached spreadsheet details which specific data attribute is contained within the applicable Verifiable Credential. The data relates to the following major fields:

1. Notifier
2. Posted Worker Employee
3. Employer company in Germany
4. Legal representative of employer company in Germany
5. Administrative Representative who must be located in the Netherlands and acts as a representative of the German company before the Dutch authorities, as regards to the PWN information
6. Service recipient in the Netherlands
7. Contact person of service recipient in the Netherlands
8. Project details
9. Work location

Important is that there are a lot of PII data contained in the issued PWN (date of birth of legal and administrative representative, ...) which make employers hesitant to share the PWN form with their posted workers. The same concern applies for PWN to be shared with service recipient.

2.3.3.3 PWN request & Issuance

Current process :

To start the process for the PWN application in the Netherlands, the German employer company has to login on the Website of the Ministry of Social Affairs & Employment, either with email and password or with EHerkenning (based upon the registration with the Dutch Chamber of Commerce). The website contains an online Notification Portal (meldloket.postedworkers.nl). The employer provides all the required data related to the fields mentioned above. Once completed, the notification can be downloaded immediately from the same website by the employer. The employer can chose for the employee to receive a copy of the PWN by providing their email address. In addition, the contact person of the service recipient will receive an email notification from

noreply@mail.postedworkers.nl. They will need to visit www.postedworkers.nl, create and verify their account with a password, log in as a service recipient, and then verify the PWN via the e-Herkenning Portal.

To-be process :

The request is still made by the employer. A new process including the usage of the European Business Wallet (EBW) of the employer company to exchange data and submit the request (“triggering process”) could bring significant benefits : it does reduce the administrative burden by minimizing the data to be requested of both the employer entity and the legal representative of the entity and also ensures data quality.

Another benefit for the involved actors is that the issued PWN can be received as a Verifiable Credential in the EBW of the employer entity for document -retention puposes and for potential inspection services by relevant host country inspection services. Moreover if the employer entity agrees to it a link could be forwarded to the posted worker to download the PWN directly from the system to his personal EUDI Wallet.

2.3.3.4 PWN Verification

The posted worker now works for company B abroad (e.g. Netherlands).

Different verification/usage scenarios can be possible now:

a) Verification of the citizen’s credentials by an official authority: While the citizen is working, a representative of the relevant Dutch authority (labour and social security authority, inspection services, etc. - “Verifier”) visits the company site and wants to perform a verification.

Status quo process: The Verifier asks the posted worked for his PWN and an identity document. He receives it in paper/card format. First, the verifier checks if the identity on the PWN matches the presented identity card. He then verifies the identity card (...). To check, if the PWN is not forged, he has to check if there is a corresponding posting notification in the system.

To-be process:

a) The Verifier asks the posted worker for his PWN and an identity evidence using an EUDI compliant Verifier App (new: Business Wallet Unit). The onboarded verifier creates a request for Verifiable Presentations of PWN and PID (or subsets of these; role of the PID in the verification process to be discussed...). The Verifier’s mobile device displays a QR code and a picture of the Verifier. The posted worker compares the Verifiers face with the picture, then scans the QR code (directly out of EUDI wallt or EUDI Wallet opens now) and receives the Verifier’s request. He automatically checks if the Verifier App (EBW unit) is valid and if the Verifier is authorised to ask for the requested information. The posted person also sees (and logs) basic information about the verifier, e.g. a service number. The EUDI wallet displays all this and also the information that has been requested tp present.

The EUDI wallet then proposes fitting VCs to the user and offers Selective Disclosure options. The worker confirms the right VCs and agrees to submit them (as request/ as a whole) to the Verifier. The Verifiers device receives the VPs remotely and performs the relevant checks

(valid wallet, PWN+PID not revoked, from an authorised issuer etc.). The result is displayed to the Verifier. He can now process the data to his backend with just clicking a button. The worker receives a notification that the submission was successful (further steps, e.g. report about the results tbd as depending on the connection). (= new efficient process)

b) Verification of the citizen's credentials by the service recipient in the Netherlands

c) Verification of the employer's credentials by service recipient in the Netherlands

d) Verification of the employer's credentials by the Dutch inspection services

e) Verification of already "presented" credentials by another Relying Party

General comment: We favor/want to explore an approach with a very "flexible" handling of the PWN VC. As the PWN is issued to the the employer, the VC has to contain the data of the VC subject. The business flow for the usage is that the employee or employer from the "sending state" have to share the PWN with the service recipient. In a second step, this employer/service recipient is audited and has to share the PWN with relevant inspection services. Therefore, we favor a solution where there is no strict holder binding but - on the opposite – only a "loose" or optional binding which allows it to "copy" the PWN VC. This would grant the service recipient the possibility to share it again with another relevant entity. It should be explored how such a solution could look like (especially from a technical point of view).

2.4 Additional flows

Additional flows regarding PD A1 could be:

- Instead of using the pickup code which was sent to the requesting employer:
 - The citizen does not use the "pickup code" but wants to download the PWN as a VC using the issuer's portal. DRV provides a "customer portal" for this – there, after login and authentication, all available VCs are displayed with a link/QR code to download them into the EUDI Wallet.
 - The citizen contacts the issuer directly from his EUDI Wallet, requests a list of available VCs, and selects the relevant VC(s) to be issued – this scenario is currently on hold due to pending protocol questions.
- Revocation of the PD A1 by the issuer
- (Revocation of the PD A1 issuer's accreditation, other revocation scenarios)
- Revocation of a PD A1 not "in general" but at a certain time (e.g. in case of shortened posting period)
- Presentation of PD A1 only, check of identity and legitimate possession via other means (e.g. using physical identity card and comparison)
- Request of only a subset of PD A1 information by a Verifier according to national/business specifics/policies
- Flexible flows around "Delegation/Representation/Portability" (to be defined)

- Complementing non-wallet flows, e.g. QR code based, PDF with “embedded credential” etc.

2.5 Challenges and barriers

Many challenges have been identified for the implementation of the KYE scenario:

1. Many Member-states do not allow the issuance of third parties credentials into state-operated wallets. At best, this would provide a poor user-experience (two different wallets) and at worst would completely prevent the implementation of the use-case.
2. Agencies issuing PID and EBWID will not be ready to issue ‘real’ credentials before end of 2026. As a consequence, use-cases will only be possible using synthetic data.
3. While social security and labor inspectorates agencies are involved to validate credentials definitions and attributes, they will not be part of the We Build consortium. This will also limit the use of credentials containing real data.
4. Most of the stakeholders focus on replicating the existing processes simply by replacing some parts of the process by EUDI wallet. So, potentially, not the full benefits of EUDI wallets will be demonstrated. Most of the organizations are interested in a step-by-step approach rather than a complete shift from day1.
5. There are some interests to be able to verify all KYE credentials in a face-to-face context and even offline. This can happen during audits on fields. The offline mode will probably not be supported by most wallets and therefore left out for the initial phases.

2.6 Working Assumptions

In order to progress in the context of uncertainty, the following assumptions have been made:

1. Private wallets will be used to implement KYE scenario (eg Credenco). This will reduce the dependencies to state-operated wallets limitations and availabilities.
2. During phase1, only synthetic data will be used to demonstrate all possible benefits of the wallet ecosystem. Real data will be used in phase2 when all conditions will be fulfilled (PID, EBWID, wallets, ...)
3. The PWN credential is containing around 50 attributes depending on the member-states regulations. While the versions that will be implemented during this pilot will be validated by the specific agencies, it might vary slightly until the real implementation.

3 Roles and participants

3.1 Scenario roles and participants

Primary role	UC partner Name	Country
User of EUDI Wallet	• Employees from Bosch	DE
	• Employees from Fragomen	DE
Authentic sources	• Bosch	DE
	• Fragomen	DE
	• DRV Bund	DE
	• Spanish labor inspectorate	SP
	• Dutsch ministry of social affairs and Employment	NL
	• Finnish Center for Pensions / Register Services	FI
Relying party	• SICPA	SP
	• DRV Bund	DE
	• Bosch	DE
	• Fragomen	NL
Intermediary	• SICPA	SP
	• Spherity	DE
	• Bosch	DE

3.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	• Credenco • Walt.id	NL NL	
2. PID Provider	• RvIG	NL	
3. Trusted list registrar	• Bundesanzeiger (GER) • KVK (Netherlands) • Registradores (SPA)	DE NL SP	
4. QEAA provider	• SwissSign	AT	
5. Pub-EAA provider	• NA		
6. EAA provider	• SICPA • Bosch	SP DE	
7. QES provider	• NA		

3.3 Target country combinations

	Issuing country				
Relying Party country		DE	NL	FI	
	SP				
	NL				

3.4 Requirements

No special requirements are expected from the involved roles.

4 Attestations

4.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

4.2 Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Person Identification Data	RvIG	NL	PID rulebook
EBW-OID	EU Organization ID	Bundesanzeiger KVK Registradores	DE NL SP	EBW-OID rulebook
EUCC	EU Company Certificate	Bundesanzeiger KVK Registradores	DE NL SP	EUCC rulebook

4.3 Created attestations in the scenario

Attestation name	Short description	For Countries	Applicable domain standards
Employee credential	See chapter 2.1	NA	
A1 certificate	See chapter 2.1	DE	
Posted Worker Notification (PWN)	See chapter 2.1	NL SP	

webuild-consortium

/

BU2

Type

/

to search

Code

Issues6

Pull requests3

Agents

Actions

Projects

BU2 / Specifications / createCompanyBranch.md



miguelaguilar-bv

Update createCompanyBranch.md

a75e1eb · last month

History

437 lines (334 loc) · 46 KB

PreviewCodeBlame

Raw

WE BUILD consortium
Specification Scenario 1 – Create a Company Branch in an EU or EEA Member State
WP2 – BU2 Create Company Branch

Date : 2026-06-22

Version : 1.0 (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)

Status : final (Draft, for review, reviewed, final)

Index

[1 Introduction 3]

[1.1 Objectives of this document 3]

[1.2 Scenario introduction 3]

[2 Scenario specification 4]

[2.1 Introduction 4]

[2.2 Scenario pre-conditions 4]

[2.3 Scenario main flow 4]

[2.4 Detailed scenario flow 4]

[2.5 Scenario additional flows 4]

[2.6 Challenges and barriers 4]

[2.7 Working Assumptions 4]

[3 Roles and participants 5]

[3.1 Scenario roles and participants 5]

[3.2 Additional roles and partners 5]

[3.3 Target country combinations 5]

[3.4 Requirements 5]

[4 Attestations 6]

[4.1 Introduction 6]

[4.2 Attestations to be provided by other UCs/WGs/scenarios 6]

[4.3 Created attestations in the scenario 6]

[Annex 1 – Requirements for scenario roles 7]

[Annex 2 – <name> 11]

Introduction

Objectives of this document

This document describes the details of scenario *Create Company Branch*, as part of use case BU2 in work package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

Scenario introduction

Cross-border registration of a company branch in a Business Register in another EU or EEA Member State, using the European Digital Identity Wallet to present issued (Q)EAAs, with Business Registers acting as relying parties, and leveraging a European Business Wallet (EBW).

Legal requirements for the Registration of a Branch in another EU or EEA Member State

A branch, as defined in Directive (EU) 2017/1132, is not a separate legal person but a permanent establishment through which the foreign company conducts its activities.

Under Directive (EU) 2017/1132, as amended by Directive (EU) 2019/1151 and Directive (EU) 2025/25, the registration of a branch of a company formed in another Member State or EEA state is governed by a harmonised set of rules designed to facilitate cross-border establishment while ensuring legal certainty and transparency.

In this framework, companies that are lawfully incorporated in one EU or EEA Member State may establish a branch in another Member State, provided that they fall within the categories covered by the Directive. Following the amendments introduced by Directive (EU) 2025/25, the scope of entities covered is expanded to include not only limited liability companies, but also certain partnership forms that are properly registered and subject to disclosure requirements in their home jurisdiction. Directive (EU) 2025/25 entered into force on 30 January 2025. Member States are required to implement the Directive in national law by 31 July 2027, and to apply the new rules from 31 July 2028. These rules will apply when the Business Wallet Regulation enters into force.

A central feature of the updated regime introduced in 2019 and 2025 is the requirement for fully digital registration procedures. Member States must allow branch registration to be carried out entirely online and ensure that all information and documents relating to both the foreign company and the branch itself can be submitted electronically. The information that must be provided about the foreign company pursuant to Article 30 of Directive (EU) 2017/1132 will be covered by the EU Company Certificate (EUCC), which was introduced in Directive (EU) 2025/25 through the insertion of Article 16b into Directive (EU) 2017/1132. The EU Company Certificate must be issued by the company's home state register and is deemed to constitute sufficient evidence of the information it contains at the time of issuance.

The business register in the host country must ensure that any application for the registration of a branch is submitted by person(s) who have the legal right and authority to act on behalf of the foreign company. To support this, Directive (EU) 2025/25 introduces a common EU power of attorney (EU PoA) by adding Article 16c to Directive (EU) 2017/1132. This is a digital tool that helps authorities check whether a person is authorised to represent the company in cross-border procedures covered by the Directive, including the registration of a branch. The EU PoA allows a company to give such authorisation in a standard and recognisable format across all EU and EEA Member States.

Directive (EU) 2025/25 reinforces the "once-only" principle for cross-border procedures. Under this principle, authorities in the host Member State must, where possible, obtain the EUCC and other relevant company information directly from the company's home register through the system of interconnected registers (BRIS), rather than requiring the company to submit the same information again. The amendments to Directive (EU) 2017/1132 introduced by Directive (EU) 2025/25 entered into force on 30 January 2025 and must be implemented in national law by 31 July 2027, with the amended provisions applying from 31 July 2028. Given that Directive (EU) 2025/25 will not be applicable until mid-2028, the Create Company Branch use case will, for the purposes of this scenario, disregard the requirement to obtain the EUCC through BRIS.

Scenario documentation

The scenario is based on the following documentation:

- Regulation (EU) 2024/1183 (eIDAS 2.0) amending Regulation (EU) No 910/2014, establishing the framework for the European Digital Identity Wallet and trust

services: <https://eur-lex.europa.eu/eli/reg/2014/910> (Consolidated version)

- Directive (EU) 2017/1132 of the the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017L1132>
- Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law: <https://eur-lex.europa.eu/eli/dir/2019/1151>
- Directive (EU) 2025/25 of the European Parliament and of the Council of 19 December 2024: <https://eur-lex.europa.eu/eli/dir/2025/25> amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law: <https://eur-lex.europa.eu/eli/dir/2025/25>. This Directive introduces, among other elements, the EU Company Certificate (EUCC) and the EU Power of Attorney (EU PoA), and entered into force on 30 January 2025.
- Proposal for a Regulation on the establishment of European Business Wallets, European Commission, November 2025: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0838>
- WP2 BU2 Stock Taking document, version 1.0
- Architecture and Reference Framework (ARF) for the European Digital Identity Wallet, latest available version: <https://eudi.dev/latest/architecture-and-reference-framework-main/>

Scenario specification

Introduction

This scenario is part of Use Case BU2, Create Company Branch and is included in the Minimum Viable Product (MVP) scope. The scenario involves the use of both European Digital Identity Wallets (EUDIW) and European Business Wallets (EBW).

This scenario starts with a company's decision to begin operating in another EU or EEA Member State. To achieve this, the company chooses to create a branch rather than a subsidiary.

Because each country implements Directive (EU) 2017/1132, as amended by Directive (EU) 2019/1151 and Directive (EU) 2025/25, in national law, the registration process and requirements for creating a branch may vary depending on the legislation of each EU or EEA Member State. In addition, there are follow-up processes required to ensure that the newly established branch can operate and conduct business in the host Member State. The scenario described here focuses on a generalized process, outlining a minimal set of activities that are common across EU and EEA Member States. The sequence of activities will be implemented according to national regulations.

In this scenario, the cross-border registration process is supported by the European Digital Identity Wallet (EUDIW) and the European Business Wallet (EBW), enabling a natural person acting on behalf of the legal entity in the home Member State to present verifiable attestations related to the legal entity and the person's representation rights. These attestations are issued by trusted sources, such as Business Registers or other authorized entities, and are used by the relying party in the host Member State to process the registration request.

The registration process starts when a natural person, with a EU Power of Attorney (EU PoA) to represent the company, interacts with the Business Register in the host Member State. The representative does this by entering the eService of the Business Register in the host Member State in order to register a company branch.

Through the eService the representative uses a personal wallet to present the requested attested attributes to the business wallet of the Business Register (relying party) as part of the registration requirements for establishing a branch.

The use of interoperable digital attestations aims to streamline the registration process, reduce administrative burden, and support compliance with both national requirements and EU regulations, including the eIDAS 2.0 framework and relevant company law requirements.

The attested attributes requested by the Business Registers are issued by public sector bodies or entities representing public sector bodies, such as Business Registers or other authorized entities, or in the case of EU PoA by the foreign company themselves if they can issue QEAs.

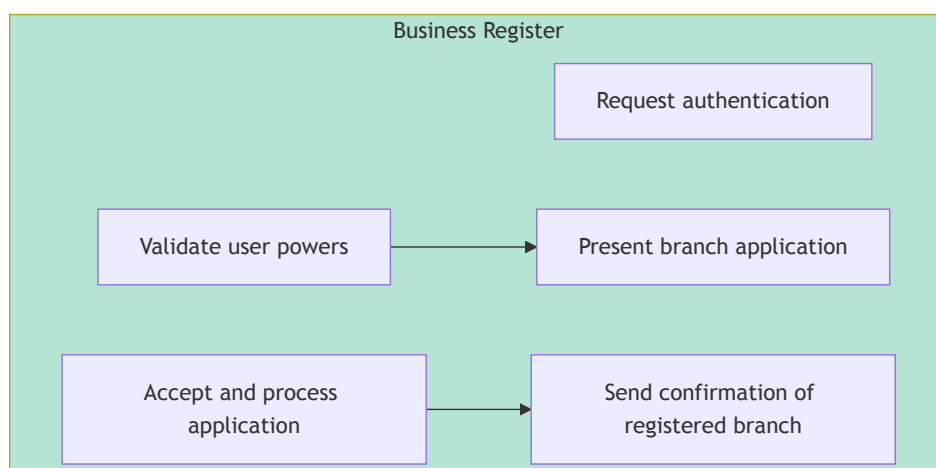
The scenario is piloted within the WE BUILD Large Scale Pilot to assess technical feasibility, interoperability, and alignment with legal requirements across Member States.

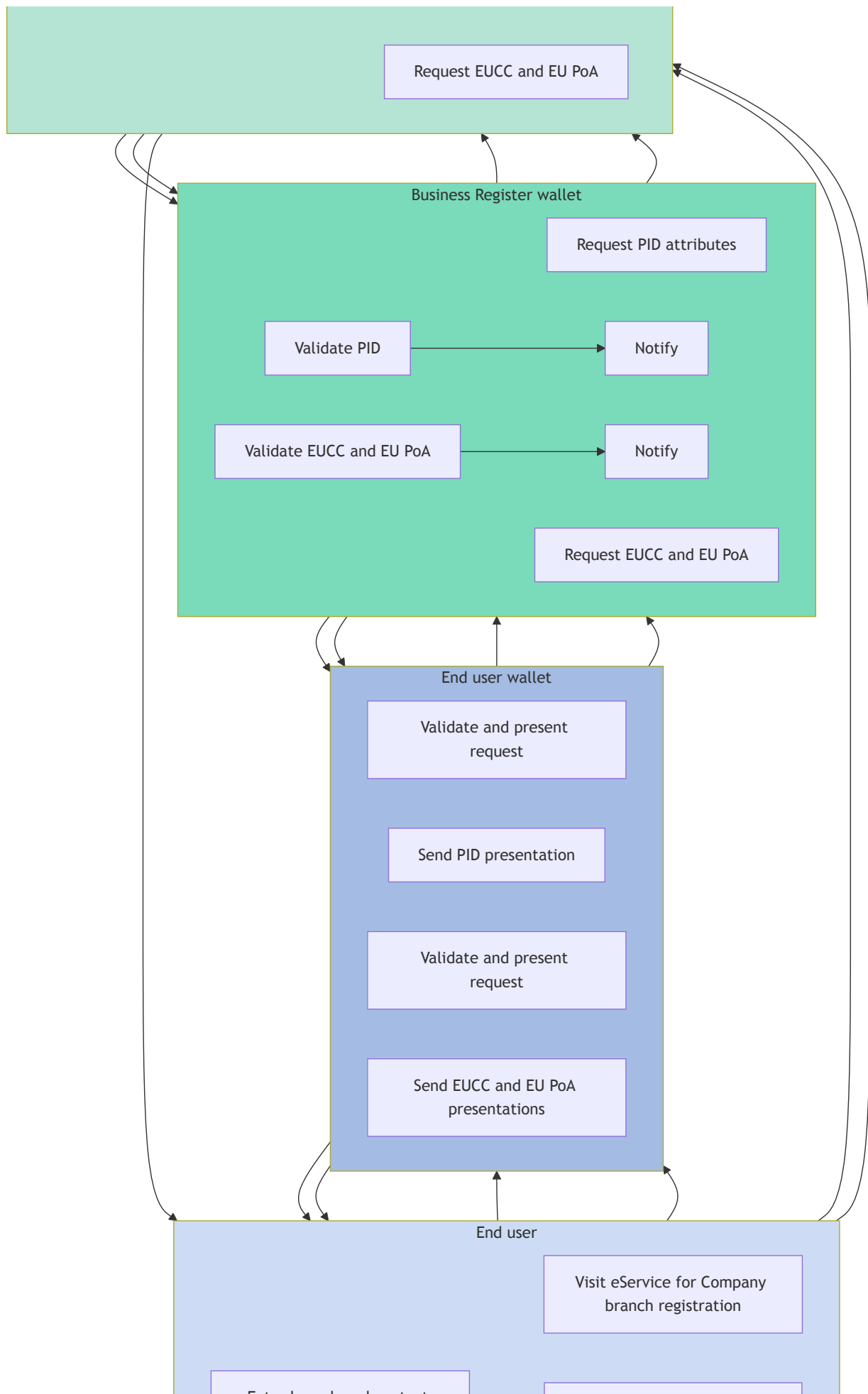
Scenario pre-conditions

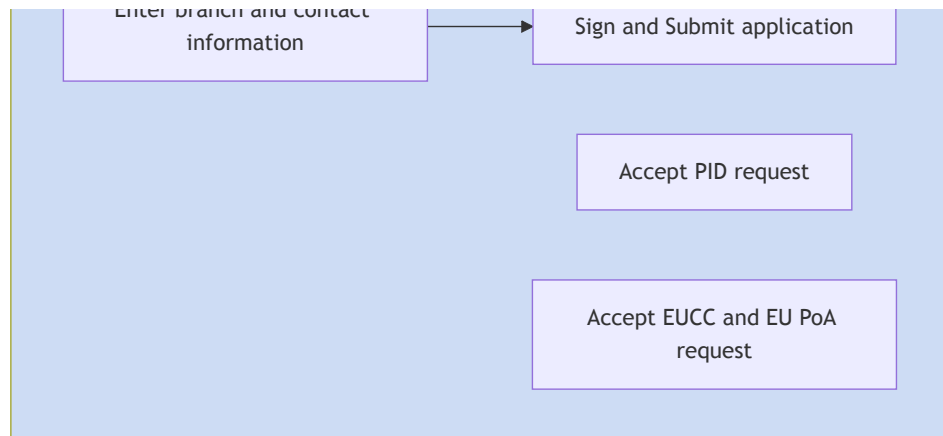
- The scenario assumes that all attestations required for the registration process have been issued and provisioned to the relevant wallets before the registration process begins. The issuance and provisioning of PID and EBWOID are provided by WE BUILD WP4. The issuance and provisioning of EUCC and EU PoA are within the scope of BU2 and will be implemented and tested by the participating authentic sources, intermediaries, and wallet providers in BU2. Issuance may be performed directly by an authentic source or through an intermediary supporting issuance service. The pilot will include testing of both attestation issuance, presentation and attestation verification to ensure end-to-end interoperability.
- The end user has acquired the attestations needed for the registration process and have them stored and available in an EUDIW. The attestations are: Person Identification Data (PID), the EU Company Certificate (EUCC) of the parent company, and an EU Power of Attorney (EU PoA) granting the end user the right to represent the parent company.
- The end user will act as the managing director of the company branch.
- Business registers have set up an eService for company branch registration.
- Business registers have acquired and stored an European Business Wallet Owner Identification Data (EBWOID) in their EBW.

Scenario main flow

As the signing authority of a registered company in an EU or EEA Member State, I want to apply to the business registry of another Member State so that I can establish a company branch.









Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Main flow step -same- device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
1. Visit eService for branch registration	End user	Natural person designated as managing director of branch visits the eService of the Business Register in the member state the foreign company wants to register a branch.		
2. Request authentication	Business Register	The Business Register requires end users to authenticate before accessing the application for branch registration. A QR code for authentication through EUDIW is		

		presented at eService. End user scans QR code with EUDIW.		
3. Request PID attributes	Business register wallet	EBW of Business Register sends request for PID attributes to end user wallet.		
4. Validate and present request	End user wallet	EUDIW of end user validates the request from EBW and presents it to end user in EUDIW.	EBWOID - WP4 PID/LPID, BWIA/BWUA - WP Wallet providers.	
5. Accept PID request	End user	End user accepts request.		
6. Send PID presentation	End user wallet	EUDIW creates presentation and sends to EBW.	PID - WP4 PID/EBWOID.	
7. Validate PID	Business Register wallet	EBW validates PID presentation.	PID - WP4 PID/EBWOID, BWIA/BWUA - WP Wallet providers.	
8. Notify	Business Register wallet	EBW sends notification to Business Register about validated PID.		
		Business Register opens eService for		

9. Request EUCC and EU PoA	Business Register	branch application to end user and requests EUCC and EU PoA by displaying QR codes for (each) attestation. End user scans code(s) with EUDIW.		
10. Request EUCC and EU PoA	Business Register wallet	EBW of Business Register sends request for EUCC and EU PoA to end user wallet.		
11. Validate and present request	End user wallet	EUDIW of end user validates the request from EBW and presents it to end user in EUDIW.	EBWOID - WP4 PID/LPID, BWIA/BWUA - WP Wallet providers.	
12. Accept EUCC and EU PoA request	End user	End user accepts request(s).		
13. Send EUCC and EU PoA presentations	End user wallet	EUDIW creates presentation(s) and sends to EBW.		
14. Validate EUCC and EU PoA	Business Register wallet	EBW validates EUCC and EU PoA.	PID - WP4 PID/EBWOID, BWIA/BWUA - WP Wallet providers.	

15. Notify	Business Register wallet	EBW sends notification to Business Register about validated presentation(s).		
16. Validate user powers	Business Register	Business Register validates that the end user has power to register branch according to EU PoA for the company of presented EUCC.		
17. Present branch application	Business Register	Business Register displays branch registration application form upon successful validation of user powers.		
18. Enter branch and contact information	End user	End user enters requested information about branch, managing director and contact information.		
				In a separate MVP+ scenario, payment

19. Sign and Submit application	End user	End user reviews application, signs and submits it to Business Register.		can be included in this step. Dependency to SCA attestation and the payment provider.
20. Accept and process application	Business Register	Business Register accepts the application and processes according to national regulation. Upon approval the branch is registered and assigned an unique identifier.		
21. Send confirmation of registered branch	Business Register	When branch is registered a confirmation (email) is sent following the contact information supplied in application form.		In an separate MVP+ scenario, QERDS can be used for notification of registration to foreign company. Dependency to EDD.

Scenario additional flows

Defined MVP+ scenarios include payment for the branch application and QERDs notifications to the company in the home Member State.

Flow	Short description
Variations	EUCC and/or EU PoA can be held in an EBW of the company.
-	
-	
Exceptions	
-	
-	
-	
-	

Challenges and barriers

Technical & Standardisation

Work Package 4 ("WP4") within the WE BUILD consortium has defined an architecture blueprint as well as conformance specifications. These technical standards, however, may not yet be stable or finalized in time for pilot implementation. The entire BU2 technical stack depends on specifications that are still evolving across multiple EU bodies, which requires coordination between BU2 and WP4.

Undefined process output

Once the registration process is completed, there is currently no fully harmonized or agreed standard at EU level defining what is issued or certified, particularly in a cross-border context. This lack of clarity could affect the role of the Business Register as an issuer, as well as the structure of the EU Company Certificate (EUCC) and the design of related attestations.

Per-jurisdiction prerequisite mapping

The BU2 scenario assumes that there is a general flow for company branch registration, and does not account for differences in national legislation and prerequisites across Member States.

Other

...

Working Assumptions

The following assumptions underpin the "Create Company Branch" scenario, focusing on cross-border registration in an EU or EEA Member State using European Business Wallets and verifiable attestations. Key assumptions include stable and comparable registration processes across Member States, full digital execution within the EU Wallet Ecosystem, presence of traceable Trust Anchors, and the ability of electronic attestations to replace physical documents with required data points. Additionally, EUDI Personal and Business Wallets operate within the same ecosystem, registration processes are clearly documented, and digital application forms are available for online completion and signing if needed.

The scenario uses only test data, excludes real user data, and focuses solely on branch creation in a second or third Member State, not the initial company registration. Processes for issuing PIDs and LPIDs, as well as architectures for QEAA issuance and qualified signing, are out of scope and are assumed to be provided by WP4. Business operations, Member State tax administration, and Ultimate Beneficiary Owner details are also excluded. The EU PoA specification is not expected until July 2026 at the earliest

Prerequisites for the scenario include an EUDI Business Wallet with user and rights management solutions, availability of PID and LPID issuers and verifiers, wallet providers supporting business wallets and wallet-to-wallet transactions, authentic sources for issuing attestations, and QTSPs capable of supporting QEAA issuance, QES/QESeal signing, Qualified Time Stamps, and QERDS implementations. Legally, agreements on scalable personal data use across the EUDI ecosystem are required, along with early synchronization of eIDAS 2.0 with GDPR, EU Data Act, data spaces regulations, AI Act, EU Data Governance Act, and related legislation.

Roles and participants

Scenario roles and participants

The following table lists per role the partners contributing within the *Create Company Branch* scenario. Additionally, the table mentions for which country the partner fulfils the role.

Primary role	UC partner name	country
1. User of EUDI Wallet	BRC	NO
	CTN, Notariado	ES
	Bolagsverket and Skatteverket	SE
	Infogreffe	FR
	KvK	NL
	Vero and PRH	FI
2. Authentic sources (issuing)	BRC	NO
	CTN, Notariado	ES
	Bolagsverket and Skatteverket	SE
	Infogreffe	FR
	KvK	NL
	Vero and PRH	FI
3. Relying party	BRC	NO
	CTN, Notariado	ES
	Bolagsverket and Skatteverket	SE
	Infogreffe	FR
	KvK	NL
	Vero and PRH	FI

4. Intermediary	iGrant.io	SE
	Credenco	NL
	D-Trust	FR
	Procivis GmbH	AT
	Siros Foundation	SE

Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	iGrant.io	SE	Data Wallet by iGrant.io
	Credenco B.V.	NL	https://docs.acc.credenco.com/
	Procivis GmbH	AT	https://docs.procivis.ch/
	Siros Foundation	SE	https://developers.siros.org/
2. PID Provider			
3. Trusted list registrar			
4. QEAA provider	D-Trust	FR	
5. Pub-EAA provider			
6. EAA provider	D-Trust	FR	
7. QES provider	D-Trust	FR	
8. European Business Wallet	iGrant.io	SE	Organisation Wallet Suite by

provider			iGrant.io
	Credenco B.V.	NL	https://docs.acc.credenco.com/
	Procivis GmbH	AT	https://docs.procivis.ch/
	Siros Foundation	SE	https://developers.siros.org/

Target country combinations

The following table states which issuing and relying party country intends to pilot the scenario of creating a company branch with each other. Specifically, issuing country I intends to pilot with relying party country R if and only if the I-R cell in the following table contains "pilot".

	Issuing country	NO	ES	SE	FR	NL	FI
Relying Party country							
NO		-	pilot	pilot			
ES			-		pilot	pilot	
SE		pilot		-		pilot	pilot
FR		pilot			-		pilot
NL		pilot			pilot	-	
FI			pilot	pilot		pilot	-

Thus, for example, the Netherlands acting as a relying party country intends to pilot with two issuing countries: France and Norway.

Requirements

The main requirements for each of the involved roles are included as an Annex.

Attestations

Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

Status per attestation and legislation

The following table presents the availability , as of March 12th 2026, per each attestation used in the BU2 scenario. "Yes" means the attestation will be available in the country represented by the column. "No" means the attestation will not be available in the country represented by the column. "Mock" means the attestation will be available, but only as mock data, in the country represented by the column.

Attestation name	FI (Vero and PRH)	FR (Infogreffe)	NL (KvK)	NO (BRC)	SE (Bolagsverket and Skatteverket)	ES (C Notari
EUCC	Yes	Yes	Yes	Yes	Yes	Yes
EU PoA	Yes	Mock	Yes	User or mock	Yes	Yes
Certificate of tax residence	Yes	No	No	No	No	Mock
VAT ID	Yes	No	No	No	Skatteverket	Mock

PID	Yes	Mock	Mock	Mock	Yes	Mock
EBWOID	Yes	Infogreffe	Yes	Yes	Yes	Mock

Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For Countries	Requirements	Rulebook reference
PID	Personal Identification Data	WP4 PID LPID	SE, FI, NL, FR, NO, ES	See rulebook	https://consortiumwebuild.github.io/attestation-catalog/pid
EBWOID	European Business Wallet Owner Identification Data	WP4 PID LPID	SE, FI, NL, FR, NO, ES	See rulebook	https://consortiumwebuild.github.io/attestation-catalog/ebwoid
Certificate of tax residence		BU3	FI		
VAT ID		BU3	SE, FI		

Created attestations in the scenario

Attestation name	Short description	For Countries	Applicable domain standards	Rulebook reference
EUCC	European Company Certificate	SE, FI, NL, FR, NO, ES	SD-JWT	https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/tree/main/rulebooks

				eucc
EU PoA	European Power of Attorney	SE, FI, NL, FR, NO, ES	SD-JWT	https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/tree/main/rulebooks/eu-poa

|

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUDI Wallet	1. The user MUST be a natural person designated by the parent company as branch representative and MUST hold a valid, machine-verifiable EU PoA issued to them by the parent company prior to starting the eService (step 3 of the detailed flow).
	2. The user MUST hold both an EUDI Personal Wallet (carrying PID, EU PoA, QES key) and an EU Business Wallet (carrying EUCC, EBWOID), pre-onboarded on the same device before the registration session.
	3. The user MUST hold a PID issued by their home Member State, at a Level of Assurance to be agreed by the BU2 partners (currently under discussion, with eIDAS LoA High as the working assumption).
	4. The user MUST be able to perform a remote QES via the EUDI Personal Wallet, including first-time QES certificate enrolment with the QTSP if not yet provisioned (step 10, including its variation).
	5. The user SHOULD be able to complete the full website to app same-device flow, and MUST also be able to complete the cross-device QR flow when the host Business Register requires it.

2. Authentic sources	1. Each authentic source MUST issue EUCC for legal entities registered in its country in SD-JWT VC format conforming to the BU2 EUCC rulebook (ds004-eucc-rulebook).
	2. Each authentic source MUST issue EBWOID for legal entities and authorised representatives registered in its country, conforming to the WP4 ds001-ebw-oid-rulebook .
	3. The authentic source for the parent-company country MUST be able to issue an EU PoA per the WP4 ds007-eu-poa-rulebook , no later than the publication date of the EU PoA specification.
	4. Each authentic source MUST publish issuer metadata to the BU2 Trusted List operated by role 7 (Trusted List registrar).
	5. Each authentic source MUST publish revocation status for EUCC, EBWOID and EU PoA via Token Status List.
	6. For attestations marked "Mock" in the availability matrix, the authentic source MUST provide functionally-equivalent mock data sufficient for end-to-end pilot testing.
3. Relying party	1. Each relying-party Business Register MUST expose a digital "Create Company Branch" eService discoverable and reachable from the natural person's home Member State.
	2. Each relying party MUST issue an OpenID4VP presentation request for the BU2 attestation set (EUCC, EBWOID, PID, EU PoA) and accept presentations in SD-JWT VC format from any of the six BU2 issuing countries listed for it in the country-pair matrix (§4.3).
	3. Each relying party MUST request and verify a remote QES over the application/declaration/notarial deed produced by the eService (steps 9 and 13 of the detailed flow).
	4. Each relying party MUST validate trust chains of received attestations against the EU Trusted Lists of all six BU2 issuing countries (SE, FI, NL, FR, NO, ES).
	5. Each relying party MUST validate the cryptographic binding linking the natural person identified by the PID, the EU PoA holder, and the legal entity referenced in the EUCC/EBWOID before

	processing the application.
	6. Each relying party MUST send a confirmation of branch registration upon successful processing; for the BU2 pilot it WON'T issue a new attestation as part of this confirmation.
	7. Each relying party SHOULD support both same-device (website to app) and cross-device (QR) wallet interaction flows, to accommodate users who arrive on either a desktop or a mobile browser.
4. Intermediary	1. MUST operate an OpenID4VP verifier endpoint that accepts presentations of the BU2 attestation set (EUCC, EBWOID, EU PoA, PID, QES) and returns a normalised verification result to the host-country Business Register backend (step 15 of the detailed flow).
	2. MUST validate trust chains against the EU Trusted Lists of all six BU2 issuing countries (SE, FI, NL, FR, NO, ES).
	3. MUST generate a tamper-evident, machine-readable data-sharing receipt (e.g. ISO/IEC 27560-aligned) for every cross-border presentation it brokers, retrievable by the natural person from the wallet UI.
	4. SHOULD provide an OpenID4VCI issuance proxy enabling Business Registers without a native issuer endpoint to issue EUCC and EU PoA in SD-JWT VC format on behalf of the authentic source.
	5. SHOULD support attestation status retrieval via Token Status List for revocation of EUCC and EU PoA issued through the proxy.
5. EUDI Wallet provider	1. MUST supply both an EUDI Personal Wallet and an EU Business Wallet instance, able to coexist on the same device, and MUST support the wallet-to-wallet hand-over of the EU PoA from the parent company's Business Wallet to the natural person's Personal Wallet.
	2. MUST support holding and presenting EUCC, EBWOID, EU PoA and PID issued by any of the six BU2 issuing countries (SE, FI, NL, FR, NO, ES), including attestations marked "Mock" in the availability matrix.

	3. MUST support OpenID4VP presentation against the relying-party Business Register in both same-device (website to app) and cross-device (QR) flows.
	4. MUST support SD-JWT VC for EUCC and EU PoA, and SHOULD additionally support mdoc to remain forward-compatible with PID/LPID variants.
	5. MUST integrate with a QTSP-backed Signature Creation Application to enable QES activation triggered by a relying-party request (steps 9 to 11 of the detailed flow).
	6. MUST validate the cryptographic binding between the EU PoA holder and the legal entity referenced in the EUCC/EBWID prior to displaying the consent UI.
	7. The wallet instance used in the pilot MUST be at Level of Assurance High per eIDAS 2.0 Article 5a.
	8. SHOULD display each presented attestation's country of issuance and trust status to the user prior to the consent gesture.
6. PID Provider	1. MUST issue machine-verifiable PIDs (in formats accepted by BU2 relying parties) with metadata that supports automated trust validation (issuer DID/keys, revocation/status endpoints, LoA).
	2. MUST publish PID issuer metadata to the BU2 Trusted List registrar (role 7) and support a Token Status List or equivalent status API for PID revocation/expiry queries.
	3. SHOULD support provisioning of PID attestations in both SD-JWT VC and mdoc-compatible formats to remain interoperable with wallet implementations.
7. Trusted list registrar	1. MUST operate and publish a BU2 Trusted List containing issuer metadata for EUCC, EBWID, EU PoA, PID and any proxy issuers, with machine-readable discovery endpoints and signed metadata.
	2. MUST provide a canonical Token Status List (or aggregated status service) indexing revocation/status sources from authentic sources, PID providers and proxy issuers, reachable by relying

	parties and intermediaries.
	3. MUST define and publish conformance requirements and onboarding procedures for issuers (including PID, QEAA/EAA proxies and QES-related services) and provide an API for registrars to push updates securely.
8. QEAA provider	1. MUST provide Qualified eIDAS Authentication Authority (QEAA) functionality where required for remote QES initiation, including authenticated session establishment between wallet and QTSP-backed Signature Creation Application.
9. Pub-EAA provider	1. MUST operate public-facing endpoints for EAA discovery (issuer metadata, public keys, verification endpoints) for any EAA instances used by the scenario and publish them to the Trusted List.
	2. MUST support issuance or hosting of verifiable EAA attestations (e.g. enterprise authentication assertions) used to bind legal-entity sessions to EU Business Wallets, with status/revocation mechanisms.
	3. SHOULD provide tooling/APIs for relying parties and intermediaries to validate EAA assertions at scale (batch/online verification) and to retrieve historical verification records if required for audit.
10. EAA provider	1. MUST issue Enterprise Authentication Assertions (EAA) that can be cryptographically bound to EU Business Wallets and referenced by relying parties to confirm entity-controlled assets or endpoints.
	2. MUST publish EAA issuer metadata and revocation/status endpoints to the Trusted List registrar and ensure keys and metadata are rotated according to BU2 security expectations.
	3. SHOULD support delegation models (e.g. service accounts, agent authorisations) so that parent companies can delegate limited EAA-based capabilities to branch representatives while preserving auditability.
11. QES	

provider	

Annex 2 – <name>

...

webuild-consortium

/

BU2

Q

+

Code

Issues6

Pull requests3

Agents

Actions

Projects

main

BU2 / Specifications / taxAuthorityRegistration.md

miguelaguilar-bv

Update taxAuthorityRegistration.md

c2d2112 · last month

423 lines (316 loc) · 39.5 KB

Preview

Code

Blame

Raw

WE BUILD consortium

Specification Scenario 2 – Registration of a Company Branch with a Tax Authority in an EU or EEA Member State

WP2 – BU2 Create Company Branch

Date : 2026-06-22

Version : 1.0 (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)

Status : final (Draft, for review, reviewed, final)

Index

[1 Introduction 3]

[1.1 Objectives of this document 3]

[1.2 Scenario introduction 3]

[2 Scenario specification 4]

[2.1 Introduction 4]

[2.2 Scenario pre-conditions 4]

[2.3 Scenario main flow 4]

[2.4 Scenario additional flows 4]

[2.5 Challenges and barriers 4]

[2.6 Working Assumptions 5]

[3 Detailed scenario flow 6]

[4 Roles and participants 7]

[4.1 Scenario roles and participants 7]

[4.2 Additional roles and partners 7]

[4.3 Target country combinations 7]

[4.4 Requirements 8]

[5 Attestations 9]

[5.1 Introduction 9]

[5.2 Attestations to be provided by other UCs/WGs/scenarios 9]

[5.3 Created attestations in the scenario 9]

[Annex 1 – Requirements for scenario roles 10]

[Annex 2 – <name> 11]

Introduction

Objectives of this document

This document describes the details of scenario *Registration of a Company Branch with a Tax Authority*, as part of use case BU2 in work package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

Scenario introduction

Cross-border registration of a company branch for Tax purposes in another EU or EEA Member State, using the European Digital Identity Wallet to present issued (Q)EAAs, with Tax Authorities acting as relying parties, and leveraging a European Business Wallet (EBW).

The scenario is based on the following documentation:

- Regulation (EU) 2024/1183 (eIDAS 2.0) amending Regulation (EU) No 910/2014, establishing the framework for the European Digital Identity Wallet and trust services
- Directive (EU) 2025/25 of the European Parliament and of the Council of 19 December 2024 amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law. This Directive introduces, among other elements, the EU Company Certificate, and entered into force on 30 January 2025.
- Proposal for a Regulation on the establishment of European Business Wallets, European Commission, November 2025: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-establishment-european-business-wallets>
- WP2 BU2 Stock Taking document, version 1.0
- Architecture and Reference Framework (ARF) for the European Digital Identity Wallet, latest available version: <https://eudi.dev/latest/architecture-and-reference-framework-main/>

Scenario specification

Introduction

This scenario is part of Use Case BU2, Create Company Branch and is included in the Minimum Viable Product (MVP) scope. The scenario involves the use of both European Digital Identity Wallets (EUDIW) and European Business Wallets (EBW).

This scenario starts with a company's decision to begin operating in another EU or EEA Member State. To achieve this, the company chooses to create a company branch rather than another legally allowed organizational form. After establishing the company branch, it will be registered for VAT with the Tax Authority.

The process and requirements to register a newly created company branch for VAT purposes vary depending on the legislation of each Member State. In addition, there are follow-up processes required to ensure that the newly created branch can operate and conduct business in the host Member State. The scenario described here focuses on a generalized process, outlining a minimal set of activities that are common across Member States. The sequence of activities will be implemented according to national regulations.

In this scenario, the cross-border registration process is supported by the European Digital Identity Wallet (EUDIW) and the European Business Wallet (EBW), enabling a natural person acting on behalf of the legal entity in the home Member State to present verifiable attestations related to the legal entity and the person's representation rights. These attestations are issued by trusted sources, such as Business Registers or other authorized entities, and are used by the relying party in the host Member State to process the registration request.

The use of interoperable digital attestations aims to streamline the registration process, reduce administrative burden, and support compliance with both national requirements and EU regulations, including the eIDAS 2.0 framework and relevant company law requirements.

The attested attributes requested by the tax authorities are issued by public sector bodies or entities representing public sector bodies, such as Business Registers or other authorized entities.

Issuance of the EU PoA depends on the final rulebook and national implementation. During the pilot, issuance may be performed by a Business Register, QTSP, notary, or the legal entity itself through issuance of a QEAA.

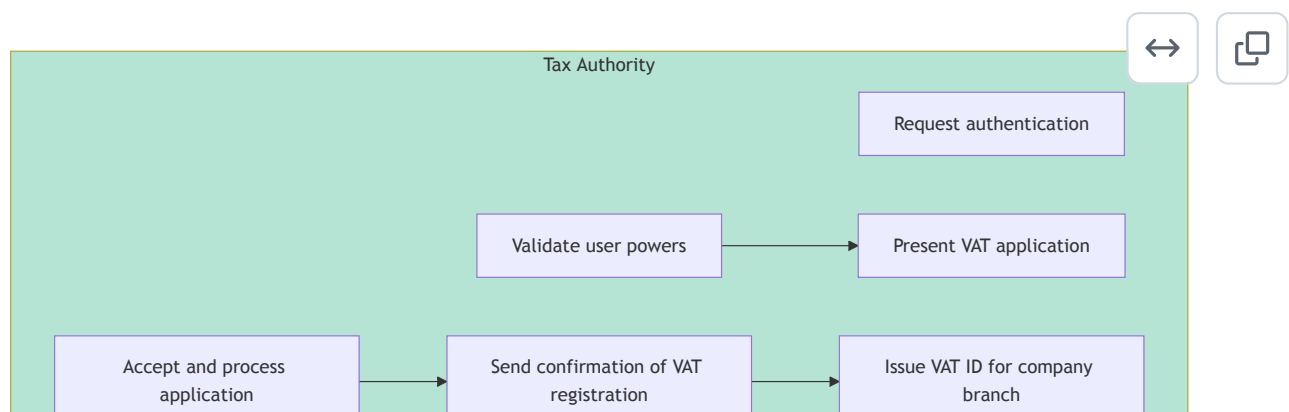
The scenario is piloted within the WE BUILD Large Scale Pilot to assess technical feasibility, interoperability, and alignment with legal requirements across Member States.

Scenario pre-conditions

- The scenario assumes that all attestations required for the registration process have been issued and provisioned to the relevant wallets before the registration process begins. The issuance and provisioning of PID and EBWOID are provided by WE BUILD WP4. The issuance and provisioning of EUCC and EU PoA are within the scope of BU2 and will be implemented and tested by the participating authentic sources, intermediaries, and wallet providers in BU2. Issuance may be performed directly by an authentic source or through an intermediary supporting issuance services. The pilot will include testing of both attestation issuance, presentation and attestation verification to ensure end-to-end interoperability.
- The end user has acquired the attestations needed for the registration process and has them stored and available in an EUDIW. The attestations are: Personal Identification Data (PID), the EU Company Certificate (EUCC) of the parent company, a VAT ID of the parent company and an EU Power of Attorney (EU PoA) granting the end user the right to represent the parent company.
- The VAT ID presented during the application process refers to the parent company in the home Member State.
- The end user will act as the managing director of the company branch.
- Tax Authorities have set up an eService for company branch VAT registration.
- Tax Authorities have acquired and stored a European Business Wallet Owner Identification Data (EBWOID) attestation in their EBW.
- The VAT ID attestation design, rulebook and schema are provided by WE BUILD BU3 and will be integrated and tested as part of the end-to-end pilot execution.

Scenario main flow

As the signing authority of a newly registered company branch, I want to register with the Tax Authority and apply for a VAT ID so that I can complete my company branch registration in another Member State.







Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Main flow step -same- device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
1. Visit eService for		Natural person designated as managing director of branch visits the eService of the Tax Authority		

VAT registration	End user	in the member state the foreign company wants to register the branch for VAT purposes.		
2. Request authentication	Tax Authority	The Tax Authority requires end users to authenticate before accessing the VAT registration application. A QR code for authentication through EUDIW is presented at eService. End user scans QR code with EUDIW.		
3. Request PID attributes	Tax Authority wallet	EBW of Tax Authority sends request for PID attributes to end user wallet.		
4. Validate and present request	End user wallet	EUDIW of end user validates the request from EBW and presents it to end user in EUDIW.	EBWOID - WP4 PID/LPID, BWIA/BWUA - WP Wallet providers.	
5. Accept PID request	End user	End user accepts request.		
6. Send PID	End user	EUDIW creates	PID - WP4	

	presentation	wallet	presentation and sends to EBW.	PID/EBWID.	
	7. Validate PID	Tax Authority wallet	EBW validates PID presentation.	PID - WP4 PID/EBWID, BWIA/BWUA - WP Wallet providers.	
	8. Notify	Tax Authority wallet	EBW sends notification to Tax Authority about validated PID.		
	9. Request EUCC, VAT ID and EU PoA	Tax Authority	Tax Authority opens eService for VAT registration to end user and requests EUCC, VAT ID and EU PoA by displaying QR codes for (each) attestation. End user scans code(s) with EUDIW.		
	10. Request EUCC, VAT ID and EU PoA	Tax Authority wallet	EBW of Tax Authority sends request for EUCC, VAT ID and EU PoA to end user wallet.		
	11. Validate and present request	End user wallet	EUDIW of end user validates the request from EBW and presents it to end user in	EBWID - WP4 PID/LPID, BWIA/BWUA - WP Wallet providers.	

		EUDIW.		
12. Accept EUCC, VAT ID and EU PoA request	End user	End user accepts request(s).		
13. Send EUCC, VAT ID and EU PoA presentations	End user wallet	EUDIW creates presentation(s) and sends to EBW.		
14. Validate EUCC, VAT ID and EU PoA	Tax Authority wallet	EBW validates EUCC, VAT ID and EU PoA.	PID - WP4 PID/EBWID, BWIA/BWUA - WP Wallet providers.	
15. Notify	Tax Authority wallet	EBW sends notification to Tax Authority about validated presentation(s).		
16. Validate user powers	Tax Authority	Tax Authority validates that the end user has power to represent the legal entity identified in the EUCC and associated VAT ID, according to the presented EU PoA.		
17. Present VAT	Tax	Tax Authority displays the VAT registration application form		

application form	Authority	upon successful validation of user powers.		
18. Enter branch and contact information	End user	End user enters requested information about branch, managing director and contact information.		
19. Sign and Submit application	End user	End user reviews application, signs and submits it to Tax Authority.		
20. Accept and process application	Tax Authority	Tax Authority accepts the application and processes according to national regulation. Upon approval the company branch is registered for VAT purposes and assigned a VAT ID according to national legislation.		
21. Send confirmation of VAT	Tax Authority	The Tax Authority sends a confirmation that the registration application has been successfully		

registration		processed to the contact details provided in the application.		
22. Issue VAT ID attestation for company branch	Tax Authority	Upon successful processing of the application, the Tax Authority issues a VAT ID attestation for the company branch based on the VAT ID rulebook and schema defined by WE BUILD BU3.		

Scenario additional flows

Flow	Short description
Variations	
-	
-	
Exceptions	
-	
-	
-	
-	

Challenges and barriers

Technical & Standardisation

Work Package 4 (WP4) within the WE BUILD consortium has defined an architecture blueprint as well as conformance specifications. These technical standards, however, may not yet be stable or finalized in time for pilot implementation. The BU2 technical stack depends on specifications that are still evolving across multiple EU bodies, which requires coordination between BU2 and WP4.

VAT ID Attestation Harmonisation

The MVP scenario assumes that the Tax Authority issues a VAT ID attestation for the company branch upon successful completion of the registration process. The VAT ID presented during the application process refers to the parent company in the home Member State, while the VAT ID issued as an outcome of the scenario refers to the company branch in the host Member State.

The design of the VAT ID attestation, including its rulebook and schema, is being developed within WE BUILD BU3 and is therefore treated as a dependency for this scenario. The pilot assumes that the VAT ID attestation defined by BU3 can be used to support issuance and acceptance of VAT ID attestations across participating Member States.

Per-jurisdiction prerequisite mapping

The MVP scenario assumes that there is a general flow for company branch registration as well as VAT registration, and does not account for differences in national legislation and prerequisites across Member States.

Identity and Representation matching

While the MVP scenario assumes that the end user is a known representative of the legal entity and is able to present the required attestations, cross-border identity and representation matching remains an open challenge at European level and is not addressed within the scope of this scenario.

Recognition of Representation Rights

The MVP scenario relies on the use of an EU PoA to demonstrate that a natural person has the right to act on behalf of a legal entity. However, representation rights, powers of attorney, and delegation models are governed by national legislation and business practices, which vary across Member States.

While the MVP scenario assumes that the presented EU PoA is accepted by the participating authorities, there may be legal, procedural, or organizational barriers to the recognition of such attestations in certain jurisdictions and use cases.

Other

...

Working Assumptions

The following assumptions underpin the "Registration of a Company Branch with a Tax Authority" scenario, focusing on cross-border VAT registration in an EU or EEA Member State using European Business Wallets and verifiable attestations. Key assumptions include stable and comparable tax and VAT registration processes across Member States, full digital execution within the EU Wallet Ecosystem, presence of traceable Trust Anchors, and the ability of electronic attestations to replace physical documents with required data points. Additionally, EUDI Personal and Business Wallets operate within the same ecosystem, tax and VAT registration processes are clearly documented, and digital application forms are available for online completion and signing if needed.

The scenario uses only test data, excludes real user data, and focuses solely on VAT registration for a company branch in a second or third Member State, not initial company registration. Processes for issuing PIDs and LPIDs, as well as architectures for QEAA issuance and qualified signing, are out of scope and are assumed to be provided by WP4. Business operations and Ultimate Beneficiary Owner details are excluded, while Member State tax administration specifics are assumed to align with EU regulations. The EU PoA specification is not expected until July 2026 at the earliest.

The scenario focuses solely on a company opening a company branch in another Member State and therefore excludes others such as Sole traders in order to limit the scope for the pilot.

In this MVP scenario, relying parties use a European Business Wallet to identify themselves towards the end user's wallet, to initiate presentation requests, and to validate received attestations.

Roles and participants

Scenario roles and participants

The following table defines which partner fulfils each role within the *Registration of a Company Branch with a Tax Authority* scenario.

Primary role	UC partner name	country
1. User of EUDI Wallet	Skatteverket	SE
	Vero	FI
2. Authentic sources	Skatteverket	SE
	Bolagsverket	SE
	Vero	FI
	PRH	FI
3. Relying party	Skatteverket	SE
	Vero	FI
4. Intermediary	iGrant.io	SE
	Credenco	NL
	Procivis GmbH	AT
	Siros Foundation	SE

Additional roles and partners

Primary role	UC partner Name	Country	Wallet

1. EUDI Wallet provider	iGrant.io	SE	Data Wallet by iGrant.io
	Credenco B.V.	NL	https://docs.acc.credenco.com/
	Procivis GmbH	AT	https://docs.procivis.ch/
	Siros Foundation	SE	https://developers.siros.org/
2. PID Provider			
3. Trusted list registrar			
4. QEAA provider	-	-	
5. Pub-EAA provider			
6. EAA provider	-	-	
7. QES provider	-	-	
8. European Business Wallet provider	iGrant.io	SE	Organisation Wallet Suite by iGrant.io
	Credenco B.V.	NL	https://docs.acc.credenco.com/
	Procivis GmbH	AT	https://docs.procivis.ch/
	Siros Foundation	SE	https://developers.siros.org/

Target country combinations

The following table states which issuing and relying party country intends to pilot the secnario of Tax Authority registration with each other. Specifically, issuing country I intends to pilot with relying party country R if and only if the I-R cell in the following table contains a "pilot".

	Issuing country						
Relying Party country		SE	FI	-	-	-	-
SE		-	pilot	-	-	-	-
FI		pilot	-	-	-	-	-

Requirements

The main requirements for each of the involved roles are included as an Annex.

Attestations

Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

Status per attestation and legislation

The following table presents the availability , as of March 12th 2026, per each attestation used in the BU2 scenario. "Yes" means the attestation will be available in the country represented by the column. "No" means the attestation will not be available in the country represented by the column. "Mock" means the attestation will be available, but only as mock data, in the country represented by the column.

--	--	--	--	--	--	--	--

Attestation name	FI (Vero and PRH)	SE (Bolagsverket and Skatteverket)	-	-	-	-
EUCC	Yes	Yes	-	-	-	-
EU PoA	Yes	Yes	-	-	-	-
VAT ID	Yes	Skatteverket	-	-	-	-
PID	Yes	Yes	-	-	-	-
EBWOID	Yes	Yes	-	-	-	-

Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For Countries	Requirements	Rulebook
PID	Personal Identification Data	WP4 PID LPID	SE,FI	See rulebook	https://consorti.attestatikatalog/pid
EBWOID	European Business Wallet Owner Identification Data	WP4 PID LPID	SE,FI	See rulebook	https://consorti.attestatikatalog/ebwoid
VAT ID	VAT Identification (for Parent Company)	BU3	SE,FI		

Created attestations in the scenario

			Applicable
--	--	--	------------

Attestation name	Short description	For Countries	domain standards	Rulebook reference
EUCC	European Company Certificate	SE, FI	SD-JWT	https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/tree/main/rulebooks/eucc
EU PoA	European Power of Attorney	SE, FI	SD-JWT	https://github.com/webuild-consortium/webuild-attestation-rulebooks-catalog/tree/main/rulebooks/eu-poa
VAT ID	VAT ID	SE, FI	SD-JWT	Following design from BU

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUDI Wallet	1. The user MUST be a natural person designated by the parent company as branch representative and MUST hold a valid, machine-verifiable EU PoA issued to them by the parent company prior to starting the eService (step 3 of the detailed flow).
	2. The user MUST hold both an EUDI Personal Wallet (carrying PID, EU PoA, QES key) and an EU Business Wallet (carrying EUCC, EBWOID and, where applicable, the Parent Company VAT ID), pre-onboarded on the same device before the registration session.
	3. The user MUST hold a PID issued by their home Member State, at a Level of Assurance to be agreed by the BU2 partners (currently under discussion, with eIDAS LoA High as the working assumption).

	4. The user MUST be able to perform a remote QES via the EUDI Personal Wallet, including first-time QES certificate enrolment with the QTSP if not yet provisioned (step 10, including its variation).
	5. The user SHOULD be able to complete the full website to app same-device flow, and MUST also be able to complete the cross-device QR flow when the host Tax Authority requires it.
2. Authentic sources	1. Each authentic source MUST issue EUCC for legal entities registered in its country in SD-JWT VC format conforming to the BU2 EUCC rulebook (ds004-eucc-rulebook).
	2. Each authentic source MUST issue EBWOID for legal entities and authorised representatives registered in its country, conforming to the WP4 ds001-ebw-oid-rulebook .
	3. The authentic source for the parent-company country MUST be able to issue an EU PoA per the WP4 ds007-eu-poa-rulebook , no later than the publication date of the EU PoA specification.
	4. Each authentic source MUST publish issuer metadata to the BU2 Trusted List operated by role 7 (Trusted List registrar).
	5. Each authentic source MUST publish revocation status for EUCC, EBWOID and EU PoA via Token Status List.
	6. For attestations marked "Mock" in the availability matrix, the authentic source MUST provide functionally-equivalent mock data sufficient for end-to-end pilot testing.
3. Relying party	1. Each relying-party Tax Authority MUST expose a digital "VAT registration" eService discoverable and reachable from the natural person's home Member State.
	2. Each relying party MUST issue an OpenID4VP presentation request for the BU2 attestation set (EUCC, VAT ID, EBWOID, PID, EU PoA) and accept presentations in SD-JWT VC format from any of the BU2 issuing countries listed for it in the country-pair matrix (§4.3).
	3. Each relying party MUST request and verify a remote QES over the application/declaration/notarial deed produced by the eService

	(steps 9 and 13 of the detailed flow).
	4. Each relying party MUST validate trust chains of received attestations against the EU Trusted Lists of all BU2 issuing countries.
	5. Each relying party MUST validate the cryptographic binding linking the natural person identified by the PID, the EU PoA holder, and the legal entity referenced in the EUCC/EBWOID before processing the application.
	6. Each relying party MUST send a confirmation of the VAT registration of the company branch upon successful processing.
	7. Each relying party SHOULD support both same-device (website to app) and cross-device (QR) wallet interaction flows, to accommodate users who arrive on either a desktop or a mobile browser.
4. Intermediary	1. MUST operate an OpenID4VP verifier endpoint that accepts presentations of the BU2 attestation set (EUCC, VAT ID, EBWOID, EU PoA, PID, QES) and returns a normalised verification result to the host-country Tax Authority backend (step 12 of the detailed flow).
	2. MUST validate trust chains against the EU Trusted Lists of all BU2 issuing countries.
	3. MUST generate a tamper-evident, machine-readable data-sharing receipt (e.g. ISO/IEC 27560-aligned) for every cross-border presentation it brokers, retrievable by the natural person from the wallet UI.
	4. SHOULD provide an OpenID4VCI issuance proxy enabling the Authentic Source without a native issuer endpoint to issue EUCC, VAT ID and EU PoA in SD-JWT VC format on behalf of the authentic source.
	5. SHOULD support attestation status retrieval via Token Status List for revocation of EUCC and EU PoA issued through the proxy.
	1. MUST supply both an EUDI Personal Wallet and an EU Business

5. EUDI Wallet provider	Wallet instance, able to coexist on the same device, and MUST support the wallet-to-wallet hand-over of the EU PoA from the parent company's Business Wallet to the natural person's Personal Wallet.
	2. MUST support holding and presenting EUCC, EBWOID, EU PoA and PID issued by any of the BU2 issuing countries, including attestations marked "Mock" in the availability matrix.
	3. MUST support OpenID4VP presentation against the relying-party Tax Authority in both same-device (website to app) and cross-device (QR) flows.
	4. MUST support SD-JWT VC for EUCC and EU PoA, and SHOULD additionally support mdoc to remain forward-compatible with PID/LPID variants.
	5. MUST integrate with a QTSP-backed Signature Creation Application to enable QES activation triggered by a relying-party request (steps 9 to 11 of the detailed flow).
	6. MUST validate the cryptographic binding between the EU PoA holder and the legal entity referenced in the EUCC/EBWOID prior to displaying the consent UI.
	7. The wallet instance used in the pilot MUST be at Level of Assurance High per eIDAS 2.0 Article 5a.
	8. SHOULD display each presented attestation's country of issuance and trust status to the user prior to the consent gesture.
6. PID Provider	1. MUST issue machine-verifiable PIDs (in formats accepted by BU2 relying parties) with metadata that supports automated trust validation (issuer DID/keys, revocation/status endpoints, LoA).
	2. MUST publish PID issuer metadata to the BU2 Trusted List registrar (role 7) and support a Token Status List or equivalent status API for PID revocation/expiry queries.
	3. SHOULD support provisioning of PID attestations in both SD-JWT VC and mdoc-compatible formats to remain interoperable with wallet implementations.

7. Trusted list registrar	1. MUST operate and publish a BU2 Trusted List containing issuer metadata for EUCC, EBWID, EU PoA, PID and any proxy issuers, with machine-readable discovery endpoints and signed metadata.
	2. MUST provide a canonical Token Status List (or aggregated status service) indexing revocation/status sources from authentic sources, PID providers and proxy issuers, reachable by relying parties and intermediaries.
	3. MUST define and publish conformance requirements and onboarding procedures for issuers (including PID, QEAA/EAA proxies and QES-related services) and provide an API for registrars to push updates securely.
8. QEAA provider	1. MUST provide Qualified eIDAS Authentication Authority (QEAA) functionality where required for remote QES initiation, including authenticated session establishment between wallet and QTSP-backed Signature Creation Application.
9. Pub-EAA provider	1. MUST operate public-facing endpoints for EAA discovery (issuer metadata, public keys, verification endpoints) for any EAA instances used by the scenario and publish them to the Trusted List.
	2. MUST support issuance or hosting of verifiable EAA attestations (e.g. enterprise authentication assertions) used to bind legal-entity sessions to EU Business Wallets, with status/revocation mechanisms.
	3. SHOULD provide tooling/APIs for relying parties and intermediaries to validate EAA assertions at scale (batch/online verification) and to retrieve historical verification records if required for audit.
10. EAA provider	1. MUST issue Enterprise Authentication Assertions (EAA) that can be cryptographically bound to EU Business Wallets and referenced by relying parties to confirm entity-controlled assets or endpoints.
	2. MUST publish EAA issuer metadata and revocation/status endpoints to the Trusted List registrar and ensure keys and

	metadata are rotated according to BU2 security expectations.
	3. SHOULD support delegation models (e.g. service accounts, agent authorisations) so that parent companies can delegate limited EAA-based capabilities to branch representatives while preserving auditability.
11. QES provider	

Annex 2 – <name>

...

WE BUILD consortium

Specification

Scenario 1 – Filing VAT-declaration Using Tax Portal

WP2 – Filing VAT-Declaration Using Tax Portal

Date : June 22th, 2026
Version : 1.0
Status : Final

Index

1	Introduction	3
1.1	Objectives of this document	3
1.2	Scenario introduction	3
2	Scenario specification	5
2.1	Introduction of BU3 scenario 1: Filing VAT declaration using Tax Portal	5
2.2	Scenario pre-conditions	5
	The following specific prerequisites exist for the use case and its scenarios:	5
2.3	Scenario main flow	6
2.4	Scenario additional flows	9
2.5	Challenges and barrier	11
2.6	Working Assumptions	11
3	Detailed scenario	12
4	Roles and participants	15
4.1	Scenario roles and participants	15
4.2	Additional roles and partners	16
4.3	Target country combinations	16
4.4	Requirements	17
5	Attestations	18
5.1	Introduction	18
5.2	Attestations to be provided by other UCs/WGs/scenarios	18
5.3	Created attestations in the scenario	19
	Annex 1 – Requirements for scenario roles	20
	Annex 2 – Authorisation Registration and Attestation Retrieval Flows	21
	Annex 3 – Authorisation Registration and Attestation Retrieval Flows of Intermediary Company	24
	Annex 4 – VAT Declaration Filing through PoA Attestation	26

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 1 Filing a VAT Declaration using the Tax Portal, as part of use case BU3 Foreign Tax Declarations in work package 2 in the WE BUILD consortium. This version constitutes the generic specifications of this BU3 scenario, and is supported by the specification documents of National Tax Administrations part of this scenario. The generic specifications explain the piloted flows by BU3 in general. However, tax processes are characterised by their national context. Therefore, the participating National Tax Administrations have defined the variants of the flow they will pilot and possible deviations from the generic flow in their specification documents. The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

BU3 aims to secure, digitalise and streamline the process of (VAT) tax declaration for, and the processes of issuing tax-attestations to, (foreign) companies, intermediaries and tax administrations, either using a Tax Portal or M2M interaction. Tax Administrations must be confident that the acting persons are authorised to do so under the laws of the member state.

Scenario 1 concerns a legal representative residing in Country B that wants to file a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A. The representative can be:

- a natural person with service-based authorisation
- a natural person with rights based upon a Power of Attorney (PoA)
- a natural person from an intermediary company in Country B based on a PoA.
- a natural person from an intermediary company in Country B with service-based authorisation within the intermediary company

The goal of this scenario is that the filer of a VAT-declaration, which is an authorised natural person of a company or an intermediary company (a company that has been granted the authority to act on behalf of intermediated company for a certain scope) receives a confirmation that the Tax Administration is able to process the VAT-declaration submission. This means that the Tax Administration has verified that the filer is authorised to file the VAT-declaration and is technically able to process the VAT-declaration. The substantive audit of the VAT declaration and the payment are out of scope.

These variants are detailed in this document as subscenarios. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved. The final chapter explains what will be learned from the scenario.

The scenario is based on the following documentation:

- a. Stock Taking Document
- b. BPMNs
- c. Architecture Reference Framework (ARF) V2.9
- d. We Build Architecture & Integration Blueprint
- e. We Build Attestation Rulebooks Catalogue

2 Scenario specification

2.1 Introduction of BU3 scenario 1: Filing VAT declaration using Tax Portal

Scenario 1 concerns a legal representative residing in Country B that wants to file a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A. The legal representative is piloted in 4 variants, addressed in different sub-scenarios.

The representative can be:

- **Subscenario 1.1:** a natural person with service-based authorisation.
- **Subscenario 1.2:** a natural person with rights based upon a PoA
- **Subscenario 1.3:** a natural person from an intermediary company in Country B based upon PoA.
- **Subscenario 1.4:** a natural person from an intermediary company in Country B with service-based authorisation within the intermediary company.

Scenario 1 pilots the authorisation of the legal representative in two ways:

- **Variant 1a:** Checking a central register – in this document referred to as an authorisation register; and/or
- **Variant 1b:** Based on an authorisation attestation.

The National Tax Administrations in BU3 decide whether they will pilot scenario 1a and/or 1b for each of the subscenario's. This shall be indicated by each Tax Administration in their specifications.

Attestations to use

- a. Person Identification Data (PID)
- b. European Business Wallet Organization Identification Data (EBWOID)
- c. Power of Attorney (full legal representative of company)
- d. Service-based authorisation attestation

2.2 Scenario pre-conditions

The following specific prerequisites exist for the use case and its scenarios:

- All natural persons involved (acting on behalf of a company or an intermediary organisation) have an EUDI Wallet containing PID and authorisation proof (either PoA or service-based authorisation).
- All business involved have an EUID and a business wallet containing EBWOID.
- There are one or more attestations that covers “acting on behalf of a legal person” defined.
- Where applicable, there is an authorisation mechanism in place for the VAT ID Certificate Issuer to consult a central authorisation register to verify the authorisation of the Intermediary. This register is out of scope for WE BUILD.

2.3 Scenario main flow

The following table presents an overview of subscenario's and variants supported by BU3 in scenario 1. When we pilot variant 1b, we have specified supporting processes that are called upon by the main flow. We will specify these in the designated annexes.

Sub-scenario	Authorisation variant	Supporting Process	Flow Category
1.1 a natural person with service-based authorisation	1.1a) Central authorisation register	NA	Main
	1.1b) Authorisation attestation	b.1a) Entering and accepting an authorisation register – fully authorised person initiated. b.1b) Entering and accepting an authorisation in a trusted authorisation register – person to be Authorised initiated b.2) Retrieval of authorisation attestation at the authorisation register	Main
1.2 a natural person with rights based upon PoA	PoA	NA	Alternative
1.3 a natural person from an intermediary company in Country B based on PoA	1.3a) PoA for NP and central authorisation registration for Intermediary.	NA	Alternative
	1.3b) PoA for NP and authorisation attestation for Intermediary	b.1a) Entering and accepting an authorisation register – fully authorised person initiated (intermediary) b.1b) Entering and accepting an authorisation in a trusted authorisation register – person to be Authorised initiated (intermediary) b.3) Retrieval of authorisation attestation for the intermediary company at the authorisation register	Alternative
1.4 a natural person from an intermediary company in Country B with service-based authorisation within the intermediary company	1.4a) Authorisation attestation for NP, central authorisation registration for Intermediary	b.1a) Entering and accepting an authorisation register – fully authorised person initiated (NP) b.1b) Entering and accepting an authorisation in a trusted authorisation register – person to be Authorised initiated (NP) b.2) Retrieval of authorisation attestation at the authorisation register (NP)	Alternative
	1.4b) Authorisation attestation for NP and	b.1a) Entering and accepting an authorisation register –	Alternative

Sub-scenario	Authorisation variant	Supporting Process	Flow Category
	Intermediary	fully authorised person initiated. b.1b) Entering and accepting an authorisation in a trusted authorisation register – person to be Authorised initiated b.2) Retrieval of authorisation attestation at the authorisation register b.3) Retrieval of authorisation attestation for the intermediated company at the authorisation register	

As seen in Table above, among 4 sub-scenarios, sub-scenario 1.1 is considered as the main flow, while the others are considered the alternative flows.

Main flow 1.1a & 1.1b: Filing VAT Declaration based on authorisation

The main objective of both main flow 1.1a & 1.1b is to model a scenario where a legal representative residing in Country B wants to file a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A through Tax Portal, especially through two main focuses either a central authorisation register (1.1a), and authorisation attestation (1.1b). In other variants of the flow and how the legal representative of the intermediary files the VAT declaration with an PoA (1.2 or 1.3) or a service-based authorisation (1.4).

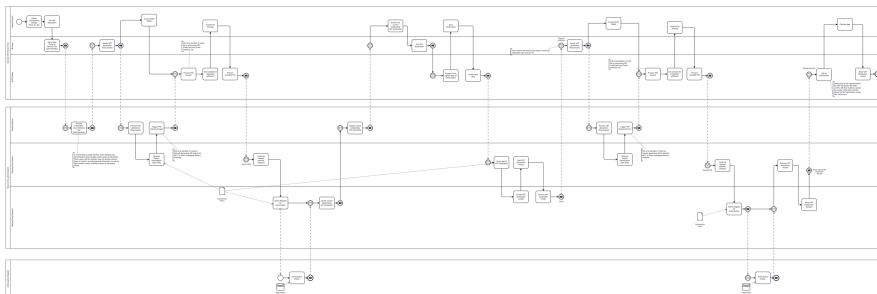
In short, the main flow is as follows: a natural person who is authorised to act as the filer of VAT declaration presents himself at the tax administration portal using an EUDI wallet. The portal uses a relying party instance to have the person identify himself with a PID. The tax administration can verify whether the person is authorised to act as the filer of VAT Declaration for the specified VAT-identified taxable person either through questioning an authorisation register directly (**Flow 1.1a**) or by requesting not only the PID but also a specific authorisation attestation for the intended action directly from the NP wallet (**Flow 1.1b**). In that case, the verification against the authorisation register is no longer required. Once confirmed, the authorised filer of VAT Declaration can file VAT Declaration for a specific company.

If supported, VAT declarations submitted through the tax administration portal can also use a Business Wallet. In this case, the European Business Wallet Organisation Identification Data (EBWOID) or another address from the Business Wallet is presented together with the Person Identification Data (PID) from the EUDI Wallet during verification. This enables the Tax Administration to send the VAT declaration receipt directly to that specific Business Wallet, in both Flows 1.1a and 1.1b.

Flow 1.1a) Filing VAT Declaration with authorisation register

Goal: a legal representative residing in Country B files a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A through Tax Portal where the authorisation is confirmed with a central authorisation register, and receives a confirmation that the Tax Administration is able to process the VAT-declaration.

A natural person who is authorised to act as the filer of VAT Declaration presents himself at the tax administration portal using a EUDI wallet. The portal uses a relying party instance to have the person identify himself with a PID. Since the personal data has already been recorded in the authorisation register, the tax administration can verify at the authorisation register whether the person is authorised to act as the filer of VAT Declaration for the specified VAT-identified taxable person. If this is confirmed, the natural person could act as the filer of VAT Declaration for the specified VAT-identified taxable person.



At this stage, there are three main actors with some sub-actors/systems as follows:

- Intended filer of VAT Declaration, which involves the Natural Person, browser, and the EUDI Wallet.
- National Tax Administration, which involves Portal Interface, Issuing Instance, Relying Party Instance, and Relying Party Back End.
- Authorisation Register

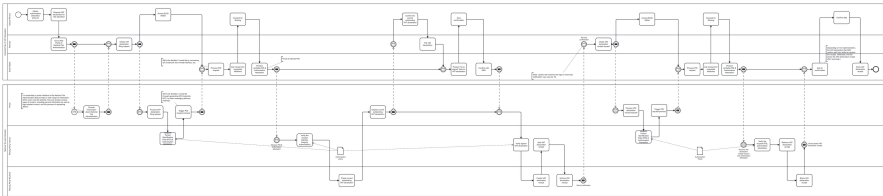
Flow 1.1b) Filing VAT Declaration with authorisation attestation

Goal: a legal representative residing in Country B files a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A through Tax Portal where the authorisation is confirmed with an authorisation attestation, and receives a confirmation that the Tax Administration is able to process the VAT-declaration.

Flow 1.1b presents an alternative model in which the tax administration requests not only the PID but also a specific authorisation for the intended action directly from the EUDI wallet. Within BU3, this specific authorisation is proven by the presentation of an authorisation attestation. In this case, the verification against the authorisation register is no longer required.

There are two ways of obtaining an authorisation attestation, either using the intermediary company, or not. If not using the intermediary company, the process of obtaining an authorisation attestation is shown in **Flow 1.1b.1 (See Annex 2)**. However, if using the

intermediary company, the process of obtaining an authorisation attestation as an intermediary is shown in **Flow b.3 (See Annex 3)**.



The actors involved in this process are as follows:

- Intended Filer of VAT Declaration, which involves the natural person, EUDI Wallet, and the browser.
- National Tax Administration, which involves Web Portal/Portal Interface, Relying Party Instance, Issuing Instance, and Back End.

2.4 Scenario additional flows

In addition to the main flows in Section 2.3 BU3 pilots more variants to enable the piloting of the subscenario’s legal representative of the company. The table below presents the flows of BU3, its variants and supporting processes.

Flow	Short description
<i>Main flow</i>	<i>Two main alternative authorisation verification patterns for VAT-declaration filing through Tax Portal.</i>
1.1a) Filing VAT Declaration with service-based authorisation from Authorisation Register	The authorised person is authorised in a register to file VAT Declaration on behalf of the specified company. The person files the VAT-declaration. In the verification process, the National Tax Administration will do the lookup to the authorisation register regarding the authorisation and processes the VAT declaration accordingly. BU3 would specifically like to pilot revocation of authorisations within its use case.
1.1b) Filing VAT Declaration with service-based Authorisation Attestation	The authorised person proves its authorisation with an authorisation attestation on behalf of a specified company. The person files the VAT-declaration. In the verification process, the National Tax Administration verifies the authorisation attestation and processes the VAT declaration accordingly. BU3 would specifically like to pilot revocation of the authorisation within its use case.
<i>Variations</i>	
1.2) VAT Declaration Filing with rights based upon a Power of Attorney	Aside of filing VAT Declaration with a service-based authorisation, the authorisation in a VAT Declaration filing could also be done with a Power of Attorney by a director of a company. This attestation is issued to the EUDI wallet of the fully authorised natural person. In the verification process, the National Tax Administration verifies the PoA and processes the VAT declaration accordingly. This process is detailed in Annex 4.
1.3) VAT Declaration Filing through an intermediary company in country B based upon a PoA	Conceptually, it is the same 1.2. However, now it is not the person from the VAT identifiable person filing the VAT declaration, but an person from an intermediary in another country. Thus, the intermediary company has to obtain an authorisation from the fully authorised person from company in country A. This can be done based on the authorisation register (1a), or based on an authorisation attestation (1b). The authorisation of the natural person is provided with an PoA. BU3 would specifically like to pilot revocation of the authorisation within its use case.
1.4) VAT Declaration Filing through an intermediary company in country B with service-based authorisation within intermediary company.	Conceptually, it is the same as 1.3. However, first, the intermediary company has to obtain authorisation from the authorised person from company in country A, and the person to be authorised within the intermediary company needs to obtain authorisation from the authorised person within the intermediary company. This can be done based on the authorisation register (1a), or based on an authorisation attestation (1b). BU3 would specifically like to pilot revocation of the authorisation within its use case.
<i>Supporting processes</i>	
b.1a The fully authorised/authorised natural person registers at the authorisation register – fully authorised person initiated.	Detailed in Annex 2. This is the first step of obtaining authorisation attestation, which the person to be authorised must be registered at the authorisation register. There are two ways of registering the person to be authorised at the authorisation register, which either initiated by the fully authorised person (this person), or by the person to be authorised themselves (b.1b). This process is relevant to implement when the fully authorised person is aware that they need to authorise someone to file VAT declaration on their behalf, so they initiate this process to later grant authorisation attestation for them.
b.1b The fully authorised/authorised natural person registers at the	Detailed in Annex 2. This process has the same purpose as b.1a but through different way. This process is initiated by the person to be authorised themselves. This process is relevant to implement when the

authorisation register – person to be authorised initiated	person to be authorised is the party who is aware first that they need authorisation from the fully authorised person to file VAT declaration on their behalf.
b.2. Retrieval of authorisation attestation at the authorisation register by authorised person.	Detailed in Annex 2. This is the process done after b.1a, or b.1b is completed. After the person to be authorised is officially registered at the authorisation register, then they become authorised person who obtains the authorisation attestation to file VAT declaration on behalf of the associated company.
b.3. Retrieval of authorisation attestation by intermediary company.	Detailed in Annex 3. This process is relevant when the VAT Declaration filing will be done by the intermediary company. To make it possible, the intermediary company first must obtain an authorisation from intermediated company by being registered in the authorisation register of the intermediated company and then obtain an authorisation attestation.
Exceptions	NA

2.5 Challenges and barrier

BU3 foresees the following challenges and barriers towards the piloting of scenario 1:

- (1.7) Specifications of scenario's are not ready in time for the participants to develop and implement.
- (1.7) Specifications of authorisation attestation are not ready in time for the participants to develop and implement.
- (new) Specifications of Identity Matching are not ready in time for the participants to develop and implement.

2.6 Working Assumptions

To be specified by National Tax Administrations

3 Detailed scenario

Per step in the main flow, a detailed description is made in the table below, both for Scenario 1.1a (authorisation register), and 1.1b (authorisation attestation):

Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Obtain authorisation attestation (Flow 1b)	VAT Declaration filer (Natural Person / Browser)	Natural Person first need to obtain authorisation attestation (See Flow b.2) , detailed in Annex 2.	Natural Person must have EUDI Wallet, and fully authorised legal/natural person has registered the authorisation change on their authorisation register. Authorisation attestation.	Alternative way to prove authorisation is by accessing a central authorisation register (1a). When the PoA is used as an authorisation, this attestation also has to be obtained first For variant 1.2: PoA is obtained by director.
Access Tax Administration Web Portal (Flow 1a, and 1b)	VAT Declaration filer (Natural Person / Browser)	It marks the start of the process, where Natural Person access the Web Portal of Tax Administration, and initiate VAT declaration filing request.		
Request and present PID (Flow 1a, and 1b)	NTA (Portal / Relying Party Instance)	Portal triggers a PID presentation request towards the EUDI Wallet. Trigger method (QR code, deeplink, or NFC) is to be determined by each piloting party. In addition, the NTA requests the authorisation proof in line with the authorisation policy.	PID	1b: Authorisation attestation also requested by TA. 1.2: PoA requested. 1.3 / 1.4: Authorisation attestation for the intermediary also requested.
	VAT Declaration filer (EUDI Wallet / Natural Person)	EUDI Wallet presents a consent screen showing the requested attributes. Natural person approves. Wallet presents the verifiable PID to the relying party instance, which cryptographically verifies the presentation (issuer trust chain, validity, holder binding).	PID, authorisation attestation, PoA	
Verify the request (Identity, Integrity,	NTA (Backend / Authorisation Register)	Relying Party Instance of Tax Administration verifies the request, which includes verifying identity and	PID Authorisation Attestation	Another way of verifying request, especially regarding authorisation is by

authorisation) (Flow 1a, and 1b)		integrity.		checking central authorisation register (Flow 1a).
		The Tax Administration verifies the service-based authorisation of the natural person in line with its authorisation policy.	Authorisation attestation	In flow 1a, the Tax Administration will check the central authorisation register in line with its authorisation policy. In flow 1b, the Tax Administration will verify the presented authorisation attestation in line with its authorisation policy.
Check and Display outstanding VAT declaration (Flow 1a, 1b)	NTA (Backend / Portal)	Backend retrieves the outstanding VAT declarations for the identified person and authorised company, and Web Portal will display it.		
File VAT declaration (Flow 1a, and 1b)	VAT Declaration filer (Natural Person / Browser)	First, Natural person has to confirm the current outstanding VAT declaration. Natural person completes the VAT declaration. Natural person verifies the data.		
	VAT Declaration filer (EUDI Wallet / Natural Person)	Natural person confirms intent to submit and approves the Qualified Electronic Signature (QES).		
Process VAT declaration (Flow 1a, 1b)	NTA (RP instance/Backend)	RP instance receives the signed VAT declaration and verifies it.		
	NTA (RP instance/Backend)	After the verification, Backend creates VAT declaration receipt, sealed by the RP instance, and then receipt is archived by Backend, until Natural Person sets the request to		

		retrieve the VAT declaration		
VAT declaration filing request	VAT Declaration filer (Natural Person / Browser)	Natural Person initiates VAT declaration filing request by presenting their PID & authorisation, requested by RP Instance. The identification and authorisation process is similar as filing a VAT declaration; Natural Person presenting their PID, and there will be verification from RP Instance regarding the identity, integrity, and authorisation.	PID Authorisation Attestation	
Share VAT Declaration Receipt	NTA (RP instance/Backend)	Once the authorisation check is done, RP Instance will retrieve VAT declaration receipt, followed by the backend sharing sealed VAT declaration receipt through RP Instance to the EUDI Wallet of Natural Person. VAT declaration receipt is then stored to the EUDI Wallet or BW.		

4 Roles and participants

4.1 Scenario roles and participants

Scenario 1 includes several relying parties: the Tax Administrations from Gipuzkoa, Finland, Norway, and Sweden. The users of EUDI and Business Wallet are mocked.

Primary role	UC partner Name	Country
1. User of EUDI Wallet	Mocked	
2. Authentic sources	Provided by other use cases.	
3. Relying party	Tax Administration	GI
	Gipuzkoa Tax Administration	FI
	Finnish Tax Administration	NO
	Norwegian Tax Administration	SE
4. Intermediary	Mocked	

4.2 Additional roles and partners

The table provides an overview of the partners involved in piloting scenario 1 in BU3. It could be that the actual partners differ in the piloting phase, depending on their availability and additional interested parties.

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	Cleverbase	NL	NW
	Digidentity	NL	
	KPN	NL	
	Digdir	NO	
	Credenco	NL	BW
2. PID Provider	Digidentity	NL	NW
	KPN	NL	
	Cleverbase	NL	
	Signicat	NO	
	Digdir	NO	
	DIGG	SE	
3. Trusted list registrar	WP4		
4. QEAA provider	Reconi	NL	NW
	Signicat	NO	
	Digidentity	NL	
	Cleverbase	NL	
5. Pub-EAA provider			
6. EAA provider			
7. QES provider	Cleverbase	NL	NW
	KPN	NL	
	Digidentity	NL	
	Signicat	NO	

Kommentert [1]: Use:
 BW = business wallet
 NW = natural person wallet
 RW = natural person wallet from reference implementation

4.3 Target country combinations

Scenario 1 involves four relying parties, all of which are Tax Administrations; Gipuzkoa, Finland, Norway, and Sweden – referred to as the Relying Party country. The Holder Country is Country A in the scenarios, where the legal representative from a company resides. At this stage, discussions are still ongoing among Gipuzkoa, Finland, Norway, and Sweden regarding the respective pilot pairings, and no final agreements have been confirmed yet. As a result, the Holder Country for cross-border piloting has not yet been determined.

Relying Party country (Tax Administration)	Holder country (representative from company in country A)			
	GI	FI	NO	SE
	GI			
	FI			
	NO			

	SE				
--	----	--	--	--	--

4.4 Requirements

The main requirements for each of the involved roles are included in the flow descriptions and Annexes.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

The following table presents the attestations to be provided by other UCs/WGs/scenarios: which consist of PID, EBW-OID, PoA, and Authorisation Attestation which involves WP2 and WP4 as seen on Table below.

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Person Identification Data (PID) is the core credential issued by Member States that digitally identifies a Natural Person is. It is used to verify Natural Person's identity across EU.	PID provider	Gipuzkoa (Spain), Finland, Norway, Sweden	The PID must contains: 1) The mandatory attributes to identify the natural person based on 2977/2024. 2) The optional attributes needed as additional information to the mandatory attributes, which varies per member state.
EBW-OID	European Business Wallet Organization Identification Data (EBWOID) is the core credential issued by Member States that digitally proves the identity of legal person/company. It acts as digital company ID to be used both for public, and private sector.	EBWOID Provider	Gipuzkoa (Spain), Finland, Norway, Sweden	The EBWOID must contains: 1) The mandatory attributes to identify the company. 2) The optional attributes needed as additional information to the mandatory attributes, which varies per member state.
PoA	Power of Attorney (PoA) is an authorisation only owned by Authorised Persons to act on behalf of a specific company, with larger scope of authorisation.	BU4	Gipuzkoa (Spain), Finland, Norway, Sweden	Defined by BU4.
Service-based authorisation attestation	Authorisation attestation is an attestation that proves natural/legal person could act on behalf of other natural/legal person for a certain service-based scope.	BU4	Gipuzkoa (Spain), Finland, Norway, Sweden	Authorisation attestation must include the service-based scope defined by the TA

5.3 Created attestations in the scenario

No attestations are created in scenario 1, since the output of this scenario is a receipt of VAT declaration that will be stored to EUDI Wallet, and it is not considered an attestation, but a business document.

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUDI Wallet	a. BU3 partners will mock users b. Must possess a valid EUDI Wallet containing at least a PID and, depending on the sub-scenario, an authorisation attestation (service-based) or a Power of Attorney (PoA).
2. Authentic sources	a. Non-specific for BU3. Scenario relies on attestations and underlying authentic sources from other use cases. - b.
3. Relying party	a. Non-specific for BU3. Must support user authentication b. Must be capable of requesting, receiving, and processing verifiable credentials, including PID, EBWOID, and authorisation attestation. c. Must assess and determine representation rights based on the presented attestations and the Tax Administrations authorisation policy. d. Must support corporate business processes and integrate with electronic signature, and seal workflows for tax processes. e. Must be able to process VAT declaration submissions including verification of the identity and integrity of the submission, creation of a sealed VAT declaration receipt, and storage of that receipt until retrieval by the filer.
4. Business Wallet Provider	a. Non-specific for BU3. Must maintain an authorisation register as specified in the Business Wallet regulation. b. Must support authorisation attestations – both for employees and for representing other organisations in flows for 1b. c. Must support
5. EUDI Wallet provider	a. Non-specific for BU3 - Must enable OpenID4VP interactions b. Non-specific for BU3 - Must verify credentials for integrity, authenticity, trust status, and revocation status c. Non-specific for BU3 - Must integrate with trusted lists and credential validation services
6. PID Provider	a. Must issue PID containing both mandatory, and optional attributes depending on Member States. Each Tax Administration defines the identity data required for scenario 1 in the specific requirements. b. Non-specific for BU3 - Must support secure PID issuance, renewal, and revocation c. Non-specific for BU3 - Must provide up-to-date status information for trust and revocation need.
7. Trusted list registrar	a. Non-specific for BU3 - Must maintain and publish trusted lists b. Non-specific for BU3 - Must ensure trust status information is available and accessible for validation purposes. c. Non-specific for BU3 - Must provide machine-readable interfaces for trusted list access and consumption.
8. QEAA provider	a. Non-specific for BU3. BU3 relies on attestations by other use cases.
9. Pub-EAA provider	a. NA
10. EAA provider	a. NA
11. QES provider	a. Non-specific for BU3 - QES must be supported to file VAT declaration b. Non-specific for BU3 – Tax Administrations must be able to seal VAT declaration receipt.

Annex 2 – Authorisation Registration and Attestation Retrieval Flows

Flow 1.1b.1a & 1.1b.1b: Entering and accepting an authorisation in a trusted authorisation register

Right after retrieving the PoA attestation, a fully authorised natural person uses an EUDI Wallet to demonstrate an authority and update the organisation's authorisations.

Three aspects are key. First, a generic register is used, which determines through an authorisation policy that the person is allowed to manage authorisations. Second, authorisation categories are not yet specified. For the BU3 use case, these would need to align with those used, but here they remain generic. Third, the update is confirmed with a qualified electronic signature via the wallet. While not always required, this adds non-repudiation and is especially valuable if the register serves external purposes, such as within a business wallet, where it can support issuing attestations.

In system-to-system interactions, entries may instead be authenticated using a qualified electronic seal. If the register is part of a business wallet or operated by a trusted third party, it may also include authorisations for individuals who can manage it for specific services. This enables a layered, hierarchical authorisation model.

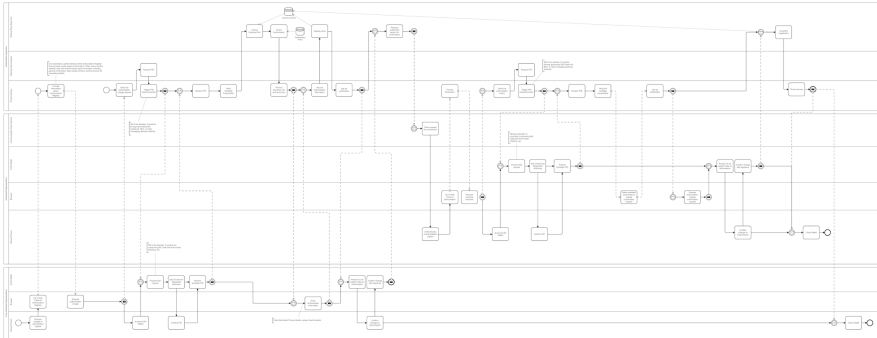
There are **two ways** of putting an entry to the authorisation register, such as:

- **b.1a)** Fully authorised person registers authorisation, and authorised person accepts
- **b.1b)** Person to be authorised registers authorisation authorisation, and fully authorised person accepts

NB, this Flow could also be implemented within the intermediary company. For instance, if the fully authorised natural person within the intermediary company needs person to be authorised to file VAT Declaration on behalf on themselves, they could enter the authorisation change to be soon accepted by the person to be authorised. The other way around process could also be done where the person to be authorised requests for the authorisation change in the authorisation register and the fully authorised person then accepts it.

However, first, the fully authorised person within the intermediary company has to obtain authorisation change/authorisation attestation from the intermediated company to do that.

b.1a) fully authorised person registers authorisation, authorised person "accepts"

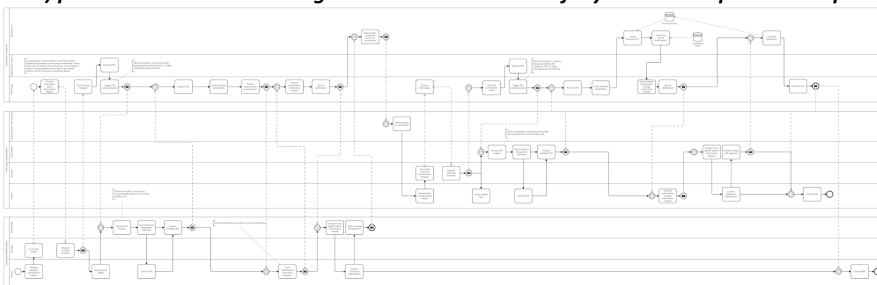


This is the first way of natural person putting an entry to the authorisation registry regarding the authorisation. This way is possible when the fully authorised person wants person to be authorised to do the process on a behalf.

In this process, there are three main actors involved, such as:

- Fully Authorised Representative, which involves Natural Person, and EUDI Wallet
- Authorised person, which involves Natural Person, and EUDI Wallet
- Authorisation Registry, which involves Portal Interface, Relying Party Instance, and Relying Party Back End

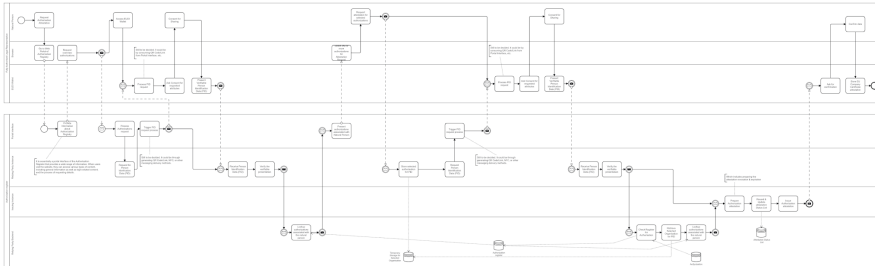
b.1b) person to be authorised registers authorisation and fully authorised person accepts.



This process is the other option for the authorised person to obtain the authorisation from the fully authorised person. However, for this way, instead of fully authorised person giving authorisation to authorised person, the authorised person requests for that authorisation to the fully authorised person.

The main and sub-actors involved are same as those involved in **1.1b.1a** process.

b.2: Retrieval of authorisation attestation at the authorisation register



This flow is executed to retrieve an authorisation attestation necessary for **Flow 1.1b**. In **Flow 1.1b**, we use an authorisation attestation as proof of authorisation to file VAT Declaration. The idea is that the fully authorised person obtains the authorisation attestation at the authorisation registry. This registry can have multiple forms, for example, it can be kept by a Tax Administration, but it could be a Business Wallet. The (fully) authorised person authenticates himself to the authorisation registry using a PID, the authorisation registry does the lookup to a system to check on the available authorisations, the (fully) authorised person selects the authorisation for attestation issuance, and the authorisation registry prepares the authorisation attestations.

For this process, there are two main actors involved such as:

- The fully authorised representatives, which involves Natural Person, and EUDI Wallet.
- The Authorisation Registry, which involves Web Portal/Portal Interface, Relying Party Instance, Issuing Instance, and Authorisation Registry Backend.

Annex 3 – Authorisation Registration and Attestation Retrieval Flows of Intermediary Company

Flow b.3: Retrieval of authorisation attestation by intermediary at the authorisation register

In Flow 1b.1, we also discuss about retrieving authorisation attestation. However, that authorisation attestation is only available for the authorised natural person working at the same company as the fully authorised natural person. It is like a boss asking for his employee to do something for him. However, in some occasions for some reasons, the intermediary company is needed to file VAT Declaration on behalf of the intermediated company.

However, in order for the intermediary company to file VAT Declaration on behalf of the intermediated company, they need to have authorisation given by the intermediated company to the intermediary, which is done through this process as follows.

This process is the same in every scenario of BU3.

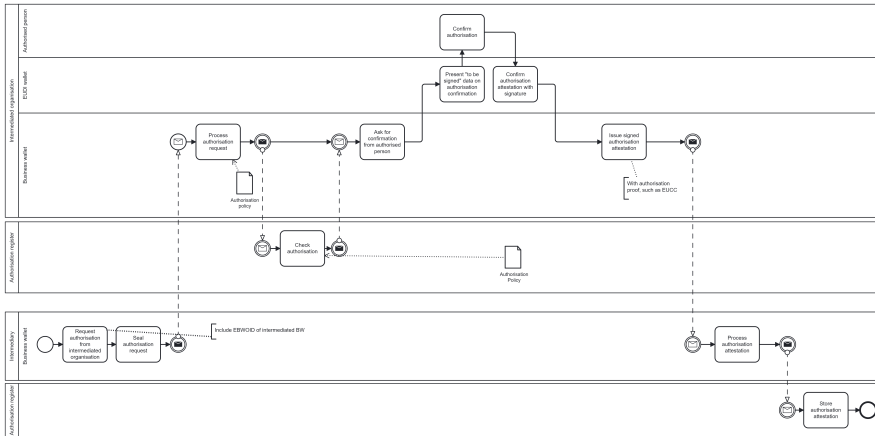
The process establishes an authorisation attestation for later use by the intermediary. The intermediary business wallet sends a sealed request to the intermediated organisation, the business wallet of the intermediated company verifies the request by accessing its authorisation register, obtains confirmation from an authorised person via the EUDI wallet, records the authorisation, and issues a signed or sealed authorisation attestation. The issued attestation is then sent back to the intermediary business wallet and stored in an authorisation register.

A prerequisite for this process is that the intermediary is registered in the authorisation register of the intermediary process. This process is explained in scenario 1 for natural persons and can be re-used for registering intermediaries.

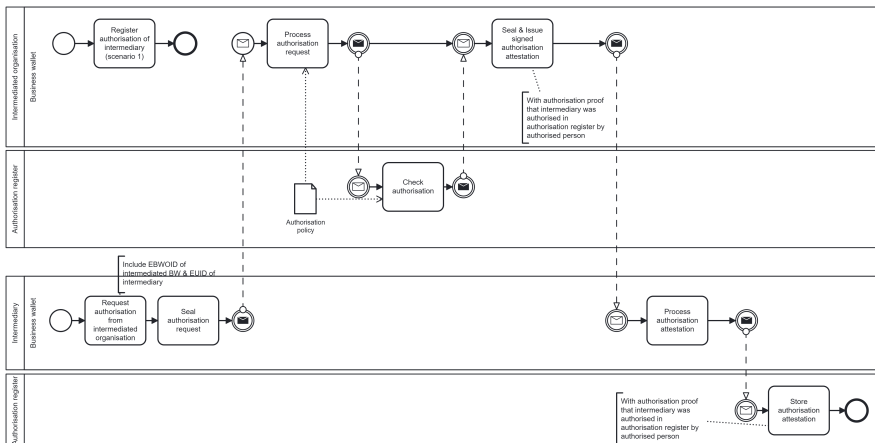
While this is not always required, the capability of an EUDI wallet makes this a highly relevant perspective. It introduces non-repudiation, which becomes particularly valuable if the register serves an external function, for example as part of a business wallet, where it can also provide a foundation for issuing attestations based on the register. This effectively turns it into a generic function that can be reused within the business wallet (**subscenario b.3a**). In full system-to-system interactions, an entry may alternatively be considered authentic when it is sealed with a qualified electronic seal (**subscenario b.3b**).

It is therefore important to note that this register, if it becomes part of a business wallet or is operated by an external trusted party, may also contain the proof or authorisation information regarding individuals who are permitted to manage and modify the register for specific services, such as authorisation of intermediaries in their authorisation register. This way, the chain of authorisation in authorisation attestations issued to intermediaries and applied in VAT declaration or VAT ID certificate issuance processed, can be validated by the Relying Party of Issuer. This enables a layered or hierarchical authorisation model.

b.3a - Issuance of authorisation attestation with Qualified Electronic Signature



b.3b - Issuance of authorisation attestation with Qseal



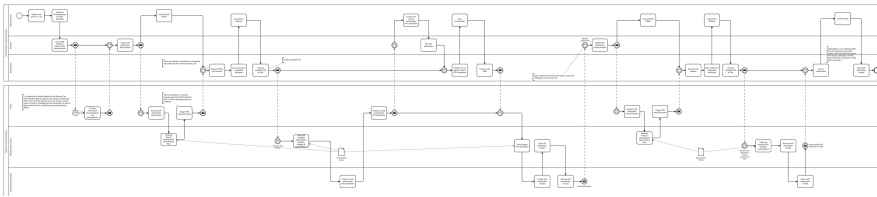
Annex 4 – VAT Declaration Filing through PoA Attestation

Flow 1.2: Authorised Person files VAT Declaration with EUDI Wallet and authorisation based upon PoA

A person who is authorised to act as the filer of VAT Declaration, the Authorised Person, obtains a PoA and presents himself at the tax administration portal using an EUDI wallet and a PoA attestation. The portal uses a relying party instance to have the person identify himself with a PID. Based on the PID and the PoA, the tax administration can verify whether the person is authorised to act as the filer of VAT Declaration. Once confirmed, the natural person could file VAT Declaration through Tax Portal.

At this stage, there are two main actors with some sub-actors/systems as follows:

- a) Intended VAT Declaration Filer, which involves Natural Person being a Authorised Person with an PoA, Browser, and EUDI Wallet.
- b) National Tax Administration, which involves Portal Interface, Relying Party Instance, and Relying Party Backend



WE BUILD consortium

Specification

Scenario 2 – Filing VAT-declaration using M2M

WP2 – Filing VAT-declaration (Using M2M Interaction)

Date	: June 22th 2026
Version	: 1.0
Status	: Final

Index

1 Introduction3

1.1 *Objectives of this document3*

1.2 *Scenario introduction3*

2 Scenario specification4

2.1 *Introduction of BU3 scenario 1: Filing VAT-declaration using M2M4*

2.2 *Scenario pre-conditions4*

2.3 *Scenario main flows4*

2.4 *Scenario additional flows8*

2.5 *Challenges and barriers10*

2.6 *Working Assumptions10*

3 Detailed scenario flow11

4 Roles and participants13

4.1 *Scenario roles and participants13*

4.2 *Additional roles and partners13*

4.3 *Target country combinations14*

4.4 *Requirements14*

5 Attestations15

5.1 *Introduction15*

5.2 *Attestations to be provided by other UCs/WGs/scenarios15*

5.3 *Created attestations in the scenario16*

Annex 1 – Requirements for scenario roles17

Annex 2 – Intermediary obtains an authorisation attestation19

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 2 Filing VAT-declaration using M2M interaction, as part of use case BU3 Foreign Tax Declaration in work package 2 in the WE BUILD consortium. This document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario. This version constitutes the generic specifications of this BU3 scenario, and is supported by the specification documents of National Tax Administrations part of this scenario. The generic specifications explain the piloted flows by BU3 in general. However, tax processes are characterised by their national context. Therefore, the participating National Tax Administrations have defined the variants of the flow they will pilot and possible deviations from the generic flow in their specification documents.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

BU3 aims to secure, digitalise and streamline the process of (VAT) tax declaration for, and the processes of issuing tax-attestations to, (foreign) companies, intermediaries and tax administrations, either using a Tax Portal or M2M interaction. Tax Administrations must be confident that the acting persons are authorised to do so under the laws of the member state. Tax Administrations want (according to the proposal of the Wallet Business regulation) to prepare for the interaction with companies and intermediary organisations (using authorisations) directly between the software of the Tax Administrations and the software of filing parties.

The objective of scenario 2 is that a business wallet of the intermediary company (a company that has been granted the authority to act on behalf of intermediated company) in country B is used to file a VAT-declaration at a Tax Administration in Country A on behalf of a company in Country A through Machine-to-Machine (M2M) Interaction. This scenario is completed when the intermediary Business wallet receives a confirmation that the Tax Administration is able to process the VAT-declaration submission. This means that the Tax Administration has verified that the filer is authorised to file the VAT-declaration and is technically able to process the VAT-declaration. The substantive audit of the VAT declaration and the payment are out of scope.

The scenario is based on the following documentation:

- Stock Taking Document
- BPMNs
- Architecture Reference Framework (ARF) V2.9
- Architecture & Integration Blueprint
- We Build Attestation Rulebooks Catalogue

2 Scenario specification

2.1 Introduction of BU3 scenario 1: Filing VAT-declaration using M2M

In short, scenario 2 concerns a business wallet of an intermediary company in country B that is used to file a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A through Machine-to-Machine (M2M) Interaction with (a business wallet) from the Tax Administration.

The scenario proves that it is possible to file a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A, using the business wallet of an intermediary company from Country B. Scenario 2 pilots the authorisation of the intermediary in two ways:

- **Scenario 2a:** Checking a central register – in this document referred to as an authorisation register.
- **Scenario 2b:** Proof of Authorisation – in this document referred to as an authorisation attestation; and/or,

The National Tax Administrations in BU3 decide whether they will pilot scenario 2a and/or 2b.

Attestations to use

- Person Identification Data (PID)
- European Business Wallet Organization Identification Data (EBWOID)
- Service-based authorisation attestation

2.2 Scenario pre-conditions

The following specific prerequisites exist for the use case and its scenarios:

- a. All natural persons involved (acting on behalf of a company or an intermediary organisation) have an EUDI Wallet containing PID
- b. All businesses involved have an EUID and a business wallet containing EBWOID.
- c. There are one or more attestations that cover “acting on behalf of a legal person” defined.
- d. The Tax Administrations have defined the service-based scope required for this scenario. Authorisation attestations must include this scope.
- e. Where applicable, there is an authorisation mechanism in place to consult a central authorisation to verify the authorisation of the Intermediary. This is out of scope for WE BUILD.

2.3 Scenario main flows

The main objective of scenario 2 is an intermediary residing in Country B wants to file a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A through Machine to Machine (M2M) with its business wallet. Scenario 2 has two main flows: Filing a VAT-declaration based on 2a) a central authorisation register, and 2b) an authorisation attestation.

The start of the flows differs, based on their authorisation mechanism, as detailed below: flow 2a starts with a check by the Intermediary BW to verify the Intermediary with the central register, flow 2b starts by obtaining an authorisation attestation. The authorisation processed are detailed under the designated flow descriptions below - the following paragraphs describe the generic process of filing a VAT-declaration that are applicable to both flows.

Filing a VAT-declaration by intermediary BW

The intermediary prepares a VAT-declaration through its Business Wallet (BW) addressed to a specific Tax Administration system. The national Tax Administrations in BU3 will either use a BW or their own specified system – both referred to as a Relying Party instances in the flows. When the national Tax Administration pilots with a BW, the request could include the EBWID or of the Tax Administration BW so that the request can be addressed and routed to the intended recipient wallet. The address should include a specification to a specified Tax Administration BW to account for the scenario where one Relying Party has multiple BWs. The Intermediary BW includes its own identification (EBWID), the identification of the intermediated company, and, in the case of flow 2b, the intermediary's authorisation attestations.

The VAT-declaration filing is then protected with the intermediary's seal. More precisely, the request carries a qualified electronic seal of the intermediary legal entity, allowing the Tax Administration Relying Party instance to verify the origin and integrity of the VAT-declaration payload. Where required by national law, the filing is confirmed by an authorised person with a qualified electronic signature.

In general, the following requirements apply:

- The Intermediary BW can file a VAT-declaration with a specified Tax Administration Relying Party Instance.
- The Tax Administration Relying Party Instance can verify that the filing originates from the intermediary legal entity (e.g. via Qualified Electronic Seal, EBWID).
- The Tax Administration can verify that the intermediary is authorised to act on behalf of the intermediated company. The intermediated company must be clearly identified to be able to process the VAT-declaration.

Processing a VAT-declaration by Tax Administration

Upon receipt of the VAT-declaration, Tax Administration Relying Party Instance performs a number of verification steps, regarding the identity, and integrity, which also includes the authorisation of the intermediary, in line with its authorisation policy. The authorisation policy should be defined by the National Tax Administrations.

The Tax Administration also performs a technical validation of the submitted VAT declaration format. To successfully pass this validation, the declaration must comply with the technical specifications of the Tax Administration. Once the validation is completed successfully, the Tax Administration generates, seals and archives the VAT declaration receipt, which serves as proof that the VAT declaration has been accepted for further processing. The Tax

Administration sends a confirmation message to the intermediary BW. The Intermediary on its turn can retrieve the receipt. The flow is completed when the sealed VAT declaration receipt is shared with the intermediary BW.

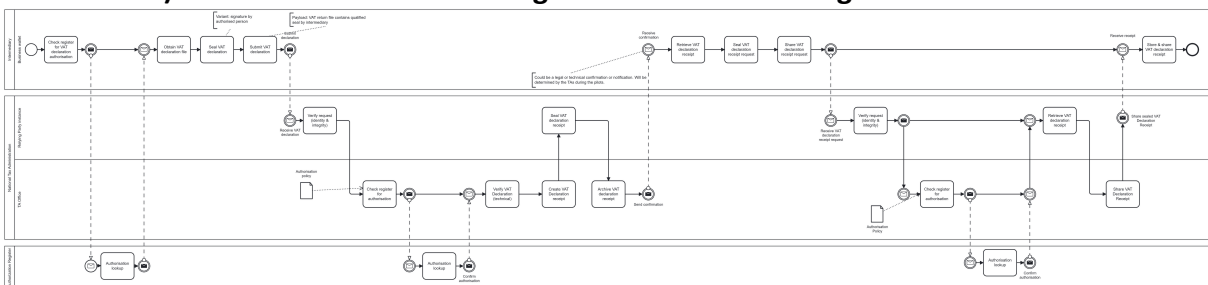
Interaction between Intermediary Business Wallet and Tax Administration

The flows intentionally abstract from the full mechanics of establishing trust between the systems. In practice, the communication setup may involve mutual authentication, certificate validation, and challenge-response steps that are not explicitly modelled here. The flows focus on the business messages specific to Scenario 2, rather than on the complete trust protocol.

Accordingly, before processing the request, the Tax Administration authenticates the Intermediary BW as a trusted communication peer. Following the WeBuild architecture, OpenID protocols is be used for requesting and issuing the VAT-ID certificate and eTRC attestations in BU3 in M2M interactions with the Business Wallet. QERDS is used for exchanging documents and notifications in BU3 in M2M interactions, specifically scenario 2 VAT declaration filing, following the WeBuild architecture. In scenario 2, attestations and documents are exchanged in one process. There are two options regarding the combination of documents: either dual-channel (file the VAT declaration using QERDS and exchange authorisation attestations using OpenID) or single-channel (filing both the document and the authorisation attestation using QERDS). The first option imposes issues when large volumes of documents are exchanged with one protocol, having to be stored temporarily while waiting for the receipt of the authorisation through another protocol. Therefore, both the document and the necessary attestations are exchanged together using QERDS in M2M interactions with the Business Wallet.

Any deviations from the WeBuild architecture by National Tax Administrations are reported in their respective scenario specifications.

Scenario 2a) M2M VAT-declaration filing with authorisation register

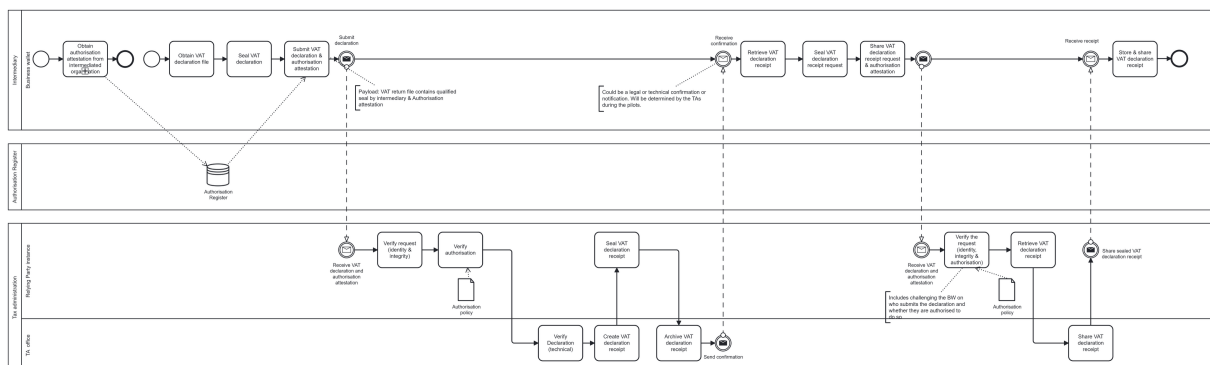


Goal: an intermediary BW in Country B files a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A through M2M where the authorisation is confirmed with a central authorisation register, and receives a confirmation that the Tax Administration is able to process the VAT-declaration.

In terms of process, in Scenario 2a, the Intermediary BW files a VAT-declaration to the Tax Administration Relying Party Instance on behalf of the intermediated company where the intermediary's authorisation is checked in a central authorisation register. The main difference compared to Scenario 2b is that the authorisation is not provided in the request itself, but is checked externally through a central authorisation register.

The intermediary validates their authorisation prior to filing the VAT-declaration with the central register of the government. The central authorisation register provides information on whether an authorisation exists, its scope (including whether it covers VAT-declaration), and whether it is still valid or has been revoked. When the Tax Administration receives the VAT-declaration, the authorisation is validated again by checking the central authorisation register. Each time an Intermediary files a VAT-declaration, the authorisation is verified.

This flow presumes the existence of a central authorisation mechanism. **Scenario 2b) M2M VAT-declaration filing with authorisation attestation**



Goal: an intermediary BW in Country B files a VAT-declaration at the Tax Administration in Country A on behalf of a company in Country A through M2M where the authorisation is confirmed with an authorisation attestation, and receives a confirmation that the Tax Administration is able to process the VAT-declaration.

Scenario 2b sets out the process by which an Intermediary BW files the VAT-declaration on behalf of an intermediated company with an authorisation attestation. This flow assumes that, prior to filing the VAT-declaration, the intermediary has obtained the necessary authorisation attestation through a separate process detailed in Annex 2.

To meet the requirement that the Tax Administration is able to verify that the Intermediary was authorised to file the VAT-declaration on behalf of the intermediated company, the Intermediary BW also shares the authorisation attestation on which it relies with the Tax Administration Relying Party Instance. Thus, the Intermediary BW includes its own identification (EBWID), VAT-declaration, and the authorisation attestation and identification of intermediated company (EUID) in the same message.

To this end, the Intermediary EBW provides the following attestations:

- The EBWID of the Intermediary, including the EUID.
- The service-based authorisation attestation, created by BU4. This contains:
 - The Intermediary EUID
 - The party concerned EUID
 - The scope:
 - referencing the VAT-declaration service

- or full scope
- Trust references Trusted issuer / Authorisation Register to validate the authorisation

Aside of performing a number of verification steps in line with its authorisation policy which includes checking the authorisation attestation issuer, integrity, validity period, and, where applicable, revocation or status information, the Tax Administration must also verify that the attestation is actually relevant to the request being processed, i.e. that it binds the identified intermediary to the intermediated company and covers the specific action of filing a VAT-declaration, or an equivalent or broader scope. Depending on the policy, the Tax Administration may require, for example, that the authorisation evidence be traceable to a natural or legal person entitled to represent the company with authorisation evidence like a seal, that the attestation contains the required representation and assurance attributes (see above), and that all trust anchors and trust service providers involved be acceptable under the Tax Administration's policy framework.

2.4 Scenario additional flows

Section 2.3 showed the main flows. However, there are more variants of to these flows, as BU3 pilots various approaches to the authorisation and required proof of the company. The table below presents the flows of BU3, its variants and supporting processes.

Flow	Short description
<i>Main flow</i>	<i>Two main alternative authorisation verification patterns for M2M VAT-declaration filing.</i>
- 2a) M2M VAT-declaration filing with authorisation register	Intermediary BW files the VAT-declaration, without presenting an attestation in the filing. The flow is completed when the Intermediary BW receives a sealed VAT-declaration receipt. The intermediary and the TA verify authorisation with the central authorisation register. BU3 would specifically like to pilot revocation of authorisations within its use case.
- 2b) M2M VAT-declaration filing with authorisation attestation	Intermediary BW files the VAT-declaration and presents a valid authorisation attestation. The flow is completed when the Intermediary BW receives a sealed VAT-declaration receipt. The Tax Administration Relying Party Instance verifies the authorisation of the Intermediary with the authorisation attestation. BU3 would specifically like to pilot revocation of authorisations within its use case.
<i>Variations</i>	
- VAT-declaration filing is confirmed with Qualified Electronic Signature of the NP submitting the filing through EUDI Wallet.	This is an alternative confirmation methods for the VAT-declaration filing. Extra flow to be piloted: Authorised person from Intermediary BW files the VAT-declaration with a qualified electronic signature from a fully authorised person through his EUDI Wallet, in addition to the Intermediary's seal. Applies to both 2a and 2b.
<i>Supporting processes</i>	
- Intermediary obtains an authorisation attestation	Detailed in Annex 2. The intermediary BW requests an authorisation attestation from the intermediated company, either sealed by the intermediated company or with the intervention of an authorised natural person that signs the authorisation attestation.
Exceptions	NA

2.5 Challenges and barriers

BU3 foresees the following challenges and barriers towards the piloting of Scenario 2:

(1.7) Specifications of scenario's are not ready in time for the participants to develop and implement

(1.7) Specifications of Authorisation attestation are not ready in time for the participants to develop and implement

(1.7) Specifications of M2M-interaction are not ready in time for the participants to develop and implement

(new) Specifications of Identity Matching are not ready in time for the participants to develop and implement

(new) Specifications for Interaction between BWs and other actors are not ready in time for the participants to develop and implement

2.6 Working Assumptions

To be specified by National Tax Administrations.

3 Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Obtain authorisation attestation from intermediated company (Scenario 2b)	Intermediary	Flow 2b-1&2, detailed in Annex 2.N	Intermediary and Intermediated companies have a BW with EBWID, EUID and the intermediated company has registered the authorisation in their authorisation register	Alternative way to prove authorisation is by accessing a central authorisation register (2a). Both the Intermediary and Tax Administration will verify the authorisation at a central register.
Fill in and submit VAT-declaration	Intermediary	To initiate the process, the intermediary first fills in and submits a VAT-declaration with address of the Tax Administration Relying Party Instance.	NA	TA may have a BW to process this filing. However, this has not been defined yet. For the generic version now, TA uses their Relying Party Instance to process this.
		VAT-declaration is sealed by intermediary	NA	
		Intermediary shares VAT-declaration and where applicable (2b) the authorisation attestation with Tax Administration	Authorisation Attestation	When using a central authorisation register (2a), only the VAT-declaration is shared.
Verify request (identity & integrity), and authorisation (2a/2b)	Tax Administration Relying Party Instance	Upon receipt of the VAT-declaration and the accompanying authorisation attestation, the Tax Administration Relying Party Instance performs a number of verification steps in line with its authorisation policy. In 2a, This includes checking the authorisation attestation issuer, integrity, validity period, and, where applicable, revocation or status information. It also verifies that the attestation is actually relevant for the VAT-declaration, while in 2b, it includes doing the lookup with the authorisation register.	NA	When using a central authorisation register (2a), the National Tax Administration consults the central authorisation register to verify the request.

Verify declaration, and create VAT declaration receipt (2a/2b)	National Tax Administration Office	The Tax Administration Office then receives and verify the VAT-declaration. It includes checking on the formatting of the submitted VAT declaration, and check whether that aligns with the formatting recognised by the system. Once finished, TA Office will create VAT declaration receipt.	NA
Seal VAT-declaration Receipt (2a/2b)	Tax Administration Relying Party Instance	Once the VAT-declaration is confirmed, TA Relying Party Instance seals the VAT-declaration receipt.	NA
Archive VAT declaration receipt (2a/2b)	Tax Administration Office	Once the receipt is sealed, the VAT declaration receipt is archived. Then, TA Office will notify Business Wallet of Intermediary to retrieve VAT declaration receipt.	NA
Retrieve, seal, and share VAT declaration receipt request (2a/2b)	Intermediary Business Wallet	This process is performed to request for VAT declaration receipt. Conceptually, it is same as when declaring VAT. This process can be fully automated – retrieving the VAT declaration receipt are mentioned separately as TAs do not always push the receipt to the VAT declaration filer.	NA
Verify authorisation, and retrieve VAT declaration receipt (2a/2b)	National Tax Administration Relying Party Instance	The Tax Administration Relying Party then receives and verifies the request. It includes checking on who submits the request and whether they are authorised to do so according to the authorisation policy. Subsequently, the TA will share sealed VAT declaration receipt.	NA
Store & share VAT-declaration receipt (2a/2b)	Intermediary Business Wallet	Once the receipt was received, the intermediary business wallet will then store and share VAT-declaration receipt.	NA

4 Roles and participants

4.1 Scenario roles and participants

This section describes the roles relevant to this scenario and lists the partners that will have this role in piloting this scenario. Three relying parties such as Tax Administrations from the Netherlands, Finland, and Norway will participate in the piloting process of this scenario. The users of EUDI and Business Wallet are mocked.

Primary role	UC partner Name	Country
1. User of EUDI Wallet	Mocked	
2. Authentic sources	Not part of BU3	
3. Relying party	Tax Administrations: Finnish Tax Administration Dutch Tax Administration Norwegian Tax Administration	FI NL NO
4. Intermediary	Mocked	

4.2 Additional roles and partners

The table provides an overview of the partners involved in BU3. It could be that the actual partners differ in the piloting phase, depending on their availability.

Primary role	UC partner Name	Country	Wallet
1. Wallet provider	Cleverbase Digidentity KPN Digdir Credenco	NL NL NL NO NL	NW BW
2. PID Provider	Digidentity KPN Cleverbase Signicat Digdir DIGG	NL NL NL NO NO SE	NW
3. Trusted list registrar	WP4		
4. QEAA provider	Reconi Signicat Digidentity	NL NO NL	BW
5. Pub-EAA provider			
6. EAA provider			
7. QES provider	Cleverbase KPN Digidentity Signicat	NL NL NL NO	NW
8. QERDS provider	Cleverbase	NL	BW

4.3 Target country combinations

Scenario 2 involves three relying parties, all of which are Tax Administrations; Finland, Netherlands, and Norway. The Holder Country is Country A in which the intermediary resides. At this stage, discussions are still ongoing among the Netherlands, Finland and Norway and available holders regarding the respective pilot pairings, and no final agreements have been confirmed yet. As a result, the Holder Country for cross-border piloting has not yet been determined.

	Holder country (representative from company in country A)			
Relying Party country (Tax Administration)		FI	NL	NO
	FI			
	NL			
	NO			

4.4 Requirements

The main requirements for each of the involved roles are included in the annexes.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

There is one attestation that will be provided by other UCs/WGs/scenarios, which is proof of authorisation which will be provided by WP2, especially BU4 as seen on Table below.

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Person Identification Data (PID) is the core credential issued by Member States that digitally identifies a Natural Person is. It is used to verify Natural Person's identity across EU.	PID Provider	Finland, Netherlands, Norway	The PID must contains: 1) The mandatory attributes to identify the natural person based on 2977/2024. 2) The optional attributes needed as additional information to the mandatory attributes, which varies per member state.
EBW-OID	European Business Wallet Organization Identification Data (EBWOID) is the core credential issued by Member States that digitally proves the identity of legal person/company. It acts as digital company ID to be used both for public, and private sector.	EBWOID Provider	Finland, Netherlands, Norway	The EBWOID must contains: 1) The mandatory attributes to identify the company. 2) The optional attributes needed as additional information to the mandatory attributes, which varies per member state.
PoA	Power of Attorney (PoA) is an authorisation only owned by fully authorised directors to act on behalf of a specific company, with unlimited scope of authorisation.	BU4	Finland, Netherlands, Norway	Defined by BU4.
Service-Based Authorisation attestation	Authorisation attestation is an attestation that proves natural/legal person could act on behalf of other natural/legal person for a certain scope.	BU4	Finland, Netherlands, Norway	Authorisation attestation must include the service-based scope defined by the TA

5.3 Created attestations in the scenario

No attestations are created in scenario 2, since the output of this scenario is a receipt of VAT declaration that will be stored in the BW; it is not considered an attestation, but a business document.

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
User of EUDI Wallet	a. BU3 partners will mock users b. In the main flows (2a, 2b), no EUDI Wallet interaction by a natural person is required. The EUDI Wallet is only used in the variation where a fully authorised person within the intermediary confirms the VAT-declaration filing with a Qualified Electronic Signature (QES). c. For the QES variation: the authorised natural person must possess a valid EUDI Wallet and must be able to approve a Qualified Electronic Signature to countersign the VAT-declaration filed by the Intermediary Business Wallet.
Authentic sources	a. Non-specific for BU3. Scenario relies on attestations and underlying authentic sources from other use cases.
Relying party	b. Non-specific for BU3. Must support user authentication, including M2M authentication of a business wallet owner. c. Must be capable of (possibly requesting), receiving, and processing verifiable credentials, including PID, EBWOID, and authorisation attestation. d. Must assess and determine representation rights based on the presented authorisation proof and the Tax Administrations authorisation policy. e. Must support corporate business processes and integrate with electronic and seal workflows for tax processes. f. Must perform technical validation of the submitted VAT-declaration format, and upon successful validation generate, seal, and archive a VAT declaration receipt and send a confirmation message to the Intermediary Business Wallet upon request. g. Optionally: must be able to operate using a Business Wallet as the Relying Party instance, enabling the incoming M2M request to be routed via EBWOID address to a specific Tax Administration BW.
Business Wallet Provider	a. Intermediary must hold a Business Wallet containing EBWOID, and must have obtained a valid authorisation from the intermediated company (either via central authorisation register (2a) or authorisation attestation (2b)) before filing a VAT-declaration on its behalf. b. Must support either the M2M authorisation verification flows: via central authorisation register (Flow 2a) and/or via authorisation attestation (Flow 2b), in accordance with the piloting choices of each National Tax Administration. c. Must be able to prepare and send a VAT-declaration filing to the Tax Administration Relying Party Instance via M2M interaction, including the identification of the intermediated company (EUID), and — in Flow 2b — the authorisation attestation. d. Must be able to retrieve the sealed VAT declaration receipt from the Tax Administration after successful processing and store it in the Intermediary Business Wallet. e. Must support piloting of revocation of authorisations, as explicitly required by BU3 for both flows 2a and 2b.
EUDI Wallet provider	a. Non-specific for BU3 - Must enable OpenID4VP interactions b. Non-specific for BU3 - Must verify credentials for integrity, authenticity, trust status, and revocation status c. Non-specific for BU3 - Must integrate with trusted lists and credential validation services
PID Provider	a. Non-specific for BU

Trusted list registrar	a.	Non-specific for BU3 - Must maintain and publish trusted lists
	b.	Non-specific for BU3 - Must ensure trust status information is available and accessible for validation purposes.
	c.	Non-specific for BU3 - Must provide machine-readable interfaces for trusted list access and consumption.
QEAA provider	d.	Non-specific for BU3. BU3 relies on attestations by other use cases.
Pub-EAA provider	a.	Non-specific for BU3.
EAA provider	a.	Non-specific for BU3.
QES provider	a.	Non-specific for BU3 - qualified sealing and optionally signing must be supported to file VAT declaration
	b.	Non-specific for BU3 – Tax Administrations must be able to seal VAT declaration receipt.

Annex 2 – Intermediary obtains an authorisation attestation

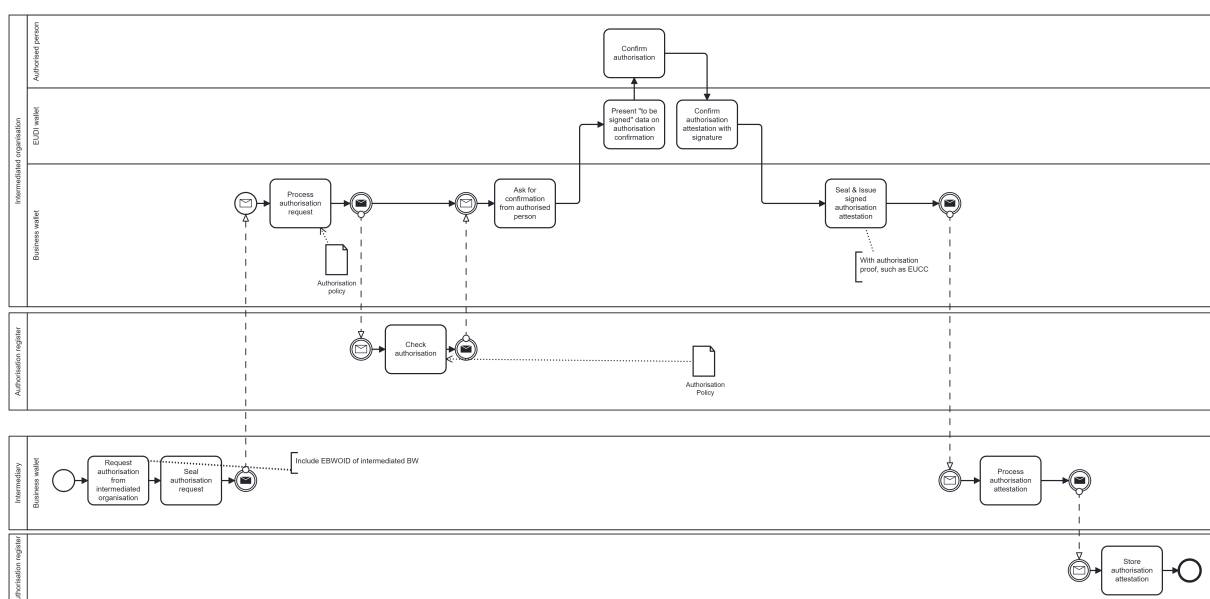
This process establishes an authorisation attestation for later use by the intermediary. The intermediary business wallet sends a sealed request to the intermediated organisation, the business wallet of the intermediated company verifies the request by accessing its authorisation register, where applicable, obtains confirmation from an authorised person via the EUDI wallet, and issues a signed and/or sealed authorisation attestation. The issued attestation is then sent back to the intermediary business wallet and stored in an authorisation register.

A prerequisite for this process is that the intermediary is registered in the authorisation register of the intermediary process. This bootstrap process is explained in scenario 1, annex 2 for natural persons and can be re-used for registering intermediaries.

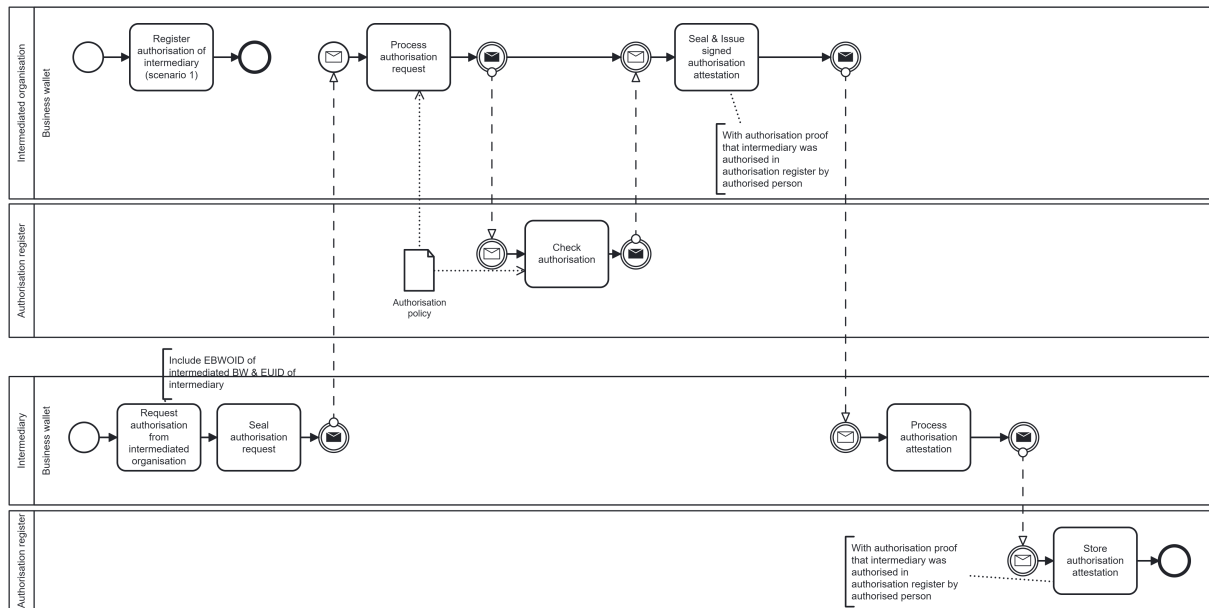
While qualified electronic signatures may not always be required, the capability of an EUDI wallet makes this a highly relevant perspective. It introduces non-repudiation, which becomes particularly valuable if the register serves an external function, for example as part of a business wallet, where it can also provide a foundation for issuing attestations based on the register. This effectively turns it into a generic function that can be reused within the business wallet (**subscenario 2b-1a**). In full system-to-system interactions, an entry may alternatively be considered authentic when it is sealed with a qualified electronic seal (**subscenario 2b-1b**).

It is therefore important to note that this register, if it becomes part of a business wallet or is operated by an external trusted party, may also contain the proof or authorisation information regarding individuals who are permitted to manage and modify the register for specific services, such as authorisation of intermediaries in their authorisation register. This way, the chain of authorisation in authorisation attestations issued to intermediaries and applied in VAT-declaration or VAT ID certificate issuance processed, can be validated by the Relying Party of Issuer. This enables a layered or hierarchical authorisation model.

Subscenario 2b-1a - Issuance of authorisation attestation with Qsig



Subscenario 2b-1b - Issuance of authorisation attestation with Qseal



WE BUILD consortium

Specification

Scenario 3 –

Issuing VAT ID

WP2 – Use Case Foreign Tax Declaration (BU3)

Date	: 22-6-2026
Version	: 1.0
Status	: Final

Index

1 Introduction3

- 1.1 Objectives of this document3*
- 1.2 Scenario introduction3*

2 Scenario specification5

- 2.1 Introduction of BU3 scenario 3: Issuing VAT ID using Tax Portal5*
- 2.2 Scenario pre-conditions5*
- 2.3 Scenario main flow6*
- 2.4 Scenario additional flows13*
- 2.5 Challenges and barriers14*
- 2.6 Working Assumptions14*

3 Detailed scenario flow15

4 Roles and participants17

- 4.1 Scenario roles and participants17*
- 4.2 Additional roles and partners17*
- 4.3 Target country combinations18*
- 4.4 Requirements18*

5 Attestations19

- 5.1 Introduction19*
- 5.2 Attestations to be provided by other UCs/WGs/scenarios19*
- 5.3 Created attestations in the scenario20*

Annex 1 – Requirements for scenario roles21

Annex 2 – Authorisation Registration and Attestation Retrieval Flows23

Annex 3 – Authorisation Registration and Attestation Retrieval Flows of Intermediary Company25

Annex 4 – Retrieval of VAT-ID Certificate with rights based upon a PoA28

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 3 Issuing VAT ID Certificate using Tax Portal (BU3), as part of use case BU3 Foreign Tax Declarations in work package 2 in the WE BUILD consortium. This version constitutes the generic specifications of this BU3 scenario, and is supported by the specification documents of National Tax Administrations part of this scenario. The generic specifications explain the piloted flows by BU3 in general. However, tax processes are characterised by their national context. Therefore, the participating National Tax Administrations have defined the variants of the flow they will pilot and possible deviations from the generic flow in their specification documents. The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

BU3 aims to secure, digitalise and streamline the process of (VAT) tax declaration for, and the processes of issuing tax-attestations to, (foreign) companies, intermediaries and tax administrations, either using a Tax Portal or M2M interaction. Tax Administrations must be confident that the acting persons are authorised to do so under the laws of the member state.

In short, this scenario concerns a legal representative residing in country B that requests from Tax Administration in Country A on behalf of a company in country A a VAT ID as an attestation. The representative can be, the same as in scenario 1:

- a natural person with service-based authorisation
- a natural person with rights based upon a Power of Attorney (PoA)
- a natural person from an intermediary company in Country B based upon PoA
- a natural person from an intermediary company in Country B with service-based authorisation within the intermediary company

The goal of this scenario is that the intended VAT ID Certificate Holder, which is an authorised natural person of a company or an intermediary company (a company that has been granted the authority to act on behalf of intermediated company for a certain scope) obtains VAT ID Certificate through Tax Portal on behalf of natural/legal person they represent. The Tax Administration issues the VAT ID certificate to the EUDI wallet or the Business wallet of the VAT ID certificate holder. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The scenario is based on the following documentation:

- Stock Taking Document
- BPMNs
- Architecture Reference Framework (ARF) V2.9
- We Build rchitecture & Integration Blueprint

- We Build Attestation Rulebooks Catalogue

2 Scenario specification

2.1 Introduction of BU3 scenario 3: Issuing VAT ID using Tax Portal

In short, scenario 3 concerns a legal representative residing in Country B wants to retrieve VAT-ID Certificate at the Tax Administration in Country A on behalf of a company in Country A. The representative can be:

- **Subscenario 3.1:** a natural person with service-based authorisation
- **Subscenario 3.2:** a natural person with rights based upon a PoA
- **Subscenario 3.3:** a natural person from an intermediary company in Country B based upon PoA.
- **Subscenario 3.4:** a natural person from an intermediary company in Country B with service-based authorisation within the intermediary company

Scenario 3 pilots the authorisation of the legal representative in two ways:

- **Variant 3a:** Checking a central register – in this document referred to as an authorisation register; and/or
- **Variant 3b:** Proof of Authorisation – in this document referred to as an authorisation attestation.

The National Tax Administrations in BU3 decide whether they will pilot scenario 3a and/or 3b for each of the subscenario's. This shall be indicated by each Tax Administration in the 1.0 version.

The attestation is issued either as a Qualified Electronic Attestation of Attributes (QEAA) or as a Public Sector Body Electronic Attestation of Attributes (PUB-EAA), and is presented to a relying party seeking a high level of assurance regarding the authenticity, integrity, and validity of the VAT identification number. The supported model shall be indicated by each National Tax Administration in the 1.0 version.

The attestation contains the EUID to which the VAT ID number is assigned, as well as the VAT identification number itself.

Attestations to use

- Person Identification Data (PID)
- European Business Wallet Organization Identification Data (EBWOID)
- Power of Attorney (full legal representative of company)
- Service-based authorisation attestation
- Value Added Tax (VAT) ID Certificate Attestation

2.2 Scenario pre-conditions

The following specific prerequisites exist for the use case and its scenarios:

- All natural persons involved (acting on behalf of a company or an intermediary organisation) have an EUDI Wallet containing PID
- All business involved have an EUID and business wallet containing EBWOID.
- There are one or more attestations that covers “acting on behalf of a legal person” defined.
- The Tax Administrations have defined the service-based scope required for this scenario. Authorisation attestations must include this scope.
- Where applicable, there is a authorisation mechanism in place in VAT ID Certificate Issuer to consult a central authorisation to verify the authorisation of the Intermediary. This register is out of scope

2.3 Scenario main flow

The following table presents an overview of subscenario’s and variants supported by BU3 in scenario 3. When we pilot variant 3b, we have specified supporting processes that are called upon by the main flow. These flows are specified these in the designated annexes.

Sub-scenario	Authorisation variant	Supporting Process	Flow Category
3.1 a natural person with service-based authorisation	3.1a) Central authorisation register	NA	Main
	3.1b) Authorisation attestation	b.1a) Entering and accepting an authorisation register – fully authorised person initiated. b.1b) Entering and accepting an authorisation in a trusted authorisation register – person to be Authorised initiated b.2) Retrieval of authorisation attestation at the authorisation register	Main
3.2 a natural person with rights based upon PoA	PoA	NA	Alternative
3.3 A natural person from an intermediary company in Country B based upon PoA	3.3a) PoA for NP and central authorisation registration for Intermediary.	NA	Alternative
	3.3b) PoA for NP and authorisation attestation for Intermediary	b.1a) Entering and accepting an authorisation register – fully authorised person initiated (intermediary) b.1b) Entering and accepting an authorisation in a trusted authorisation register – person to be Authorised initiated (intermediary) (1.3b.1) Retrieval of authorisation attestation	Alternative

		for the intermediary company at the authorisation register	
3.4 a natural person from an intermediary company in Country B with service-based authorisation within the intermediary company	3.4a) Authorisation attestation for NP, central authorisation registration for Intermediary	b.1a) Entering and accepting an authorisation register – fully authorised person initiated (NP) b.1b) Entering and accepting an authorisation in a trusted authorisation register – person to be Authorised initiated (NP) b.2) Retrieval of authorisation attestation at the authorisation register (NP)	Alternative
	3.4b) Authorisation attestation for NP and Intermediary	b.1a) Entering and accepting an authorisation register – fully authorised person initiated. b.1b) Entering and accepting an authorisation in a trusted authorisation register – person to be Authorised initiated b.2) Retrieval of authorisation attestation at the authorisation register b.3) Retrieval of authorisation attestation for the intermediated company at the authorisation register	Alternative

As seen on Table above, among above 4 sub-scenarios, sub-scenario 1.1 is considered as the the main flow, while the others are considered as alternative flows.

Flow 3.1a & 3.1b: Retrieval of VAT-ID certificate for NP wallet based on authorisation

The main objective of scenario 3.1 is that legal representative residing in Country B can retrieve VAT ID Certificate at the Tax Administration in Country A on behalf of a company in Country A through Tax Portal, both based on an service-based authorisation derived from a 3a) central authorisation register, or 3b) an authorisation attestation. In the process, we refer to “VAT ID certificate issuer” in general, to account for multiple issuing models, being the TA issuing a Pub-EAA or a QTSP issuing a QEAA VAT ID certificate. For readability, the text states Tax Administration, but as explained in 2.4, the issuer can thus also be a QTSP that retrieves or verifies attributes from the National Tax Administration Source.

The Tax Administrations must define the scope of the service-based authorisation required for this scenario. For example, the Netherlands Tax Administration may require an authorisation with service scope "VAT ID certificate request", the Bask TA may require an authorisation with service scope "Taxes". This should be defined in their authorisation policy.

A person who is authorised to act as the holder of a VAT-ID certificate presents himself at the tax administration portal using an EUDI wallet. The portal uses a relying party instance to have the person identify himself with their PID. The tax administration can verify whether the person is authorised to act as the holder of the VAT-ID certificate for the specified VAT-identified taxable person either through questioning an authorisation register directly (**Flow 3.1a**) or by requesting not only the PID but also a specific authorisation attestation for the intended action directly from the NP wallet (**Flow 3.1b**). In that case, the verification against the authorisation register is no longer required. Once confirmed, the VAT-ID certificate can be issued to the EUDI or Business Wallet in the form of an attestation .

Flow 3.1a Retrieval of VAT-ID certificate with authorisation register

Goal: a legal representative residing in Country B retrieves a VAT-ID certificate attestation at the Tax Administration in Country A on behalf of a company in Country A through Tax Portal where the authorisation is confirmed with a central authorisation register. The VAT-ID certificate is issued to either the EUDI wallet or the Business Wallet of the VAT-ID certificate holder. BU3 supports both flows presented below.

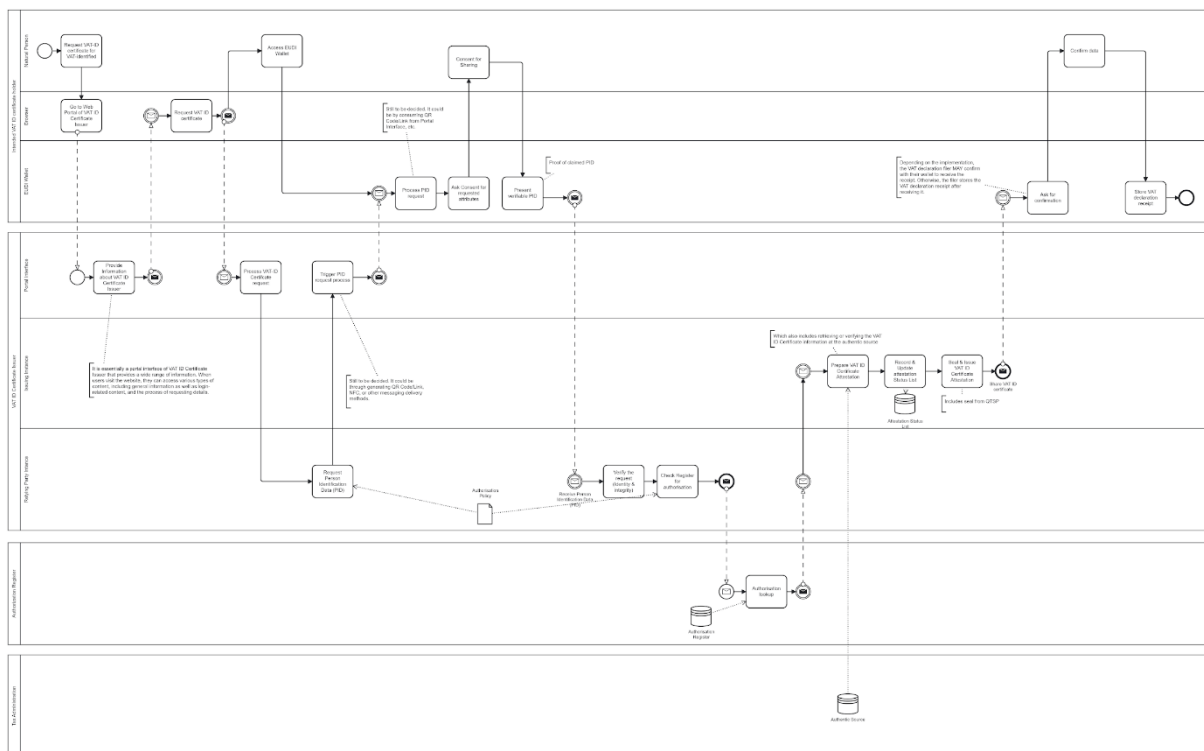
In terms of process, a person who is authorised to act as the holder of a VAT-ID certificate (the intended VAT-ID certificate holder) presents himself at the tax administration portal using an EUDI wallet. The portal uses a relying party instance to have the person identify himself with their PID. Since the personal data has already been recorded in the authorisation register, the tax administration can verify at the register whether the person is authorised to act as the holder of the VAT-ID certificate for the specified VAT-identified taxable person.

The Tax Administration will only proceed the VAT ID certificate issuance if all technical and authorisation policy checks succeed. The Tax Administration then prepares the attestation, by retrieving information from its sources (in the case of a QTSP, by retrieving or verifying attributes from the sources of the Tax Administration) and issues the VAT ID certificate attestation to either the EUDI wallet or the Business Wallet of the VAT-ID certificate holder.

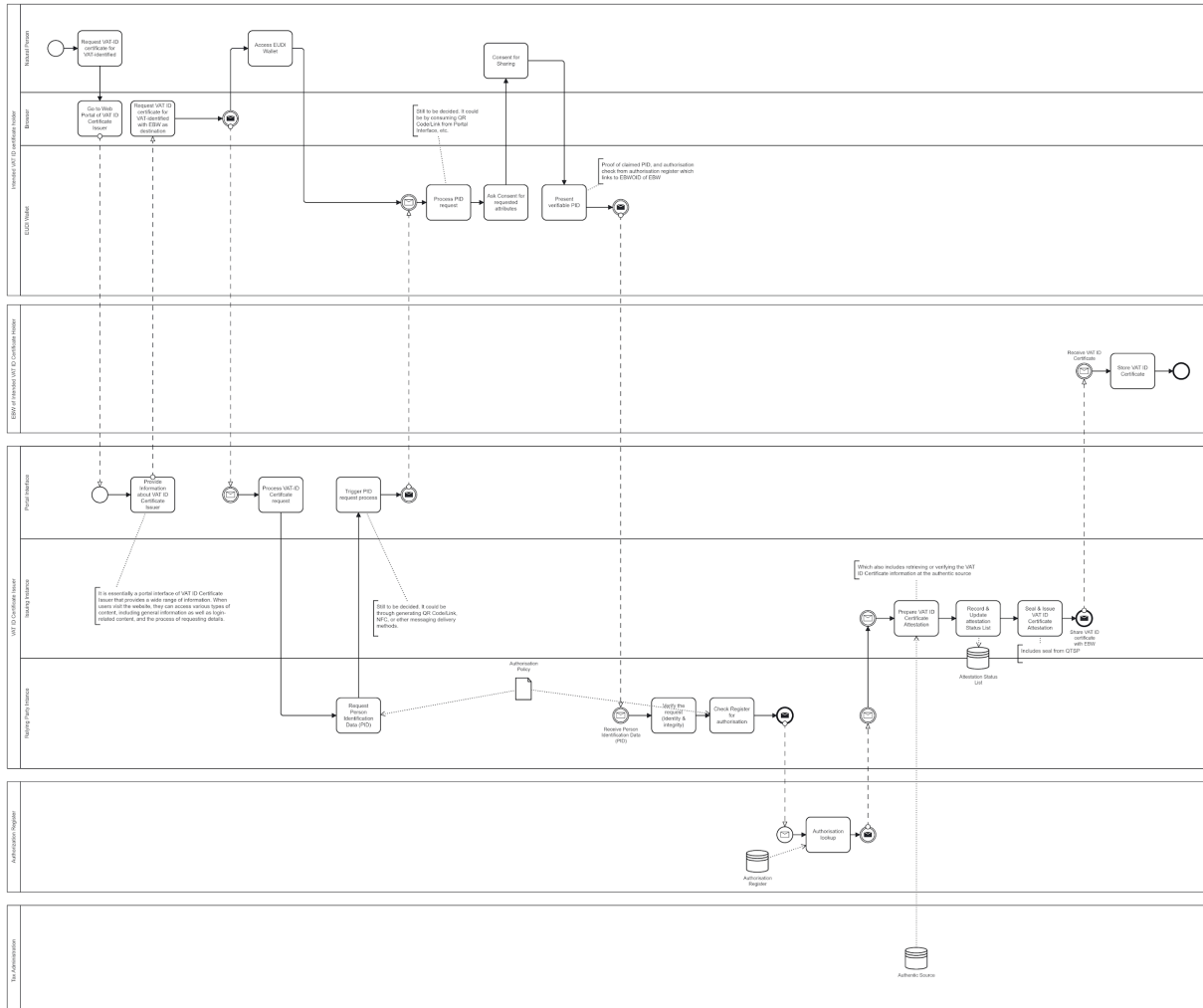
At this stage, there are four main actors with some sub-actors/systems as follows:

- Intended VAT-ID Certificate Holder, which involves the legal representative of a company, their EUDI Wallet and the Business Wallet of the company.
- VAT ID Certificate Issuer, which involves Portal Interface, Issuing Instance, Relying Party Instance, and Relying Party Back End.
- Tax Administration as authentic source
- Central Authorisation Register

1) The VAT-ID certificate holder requests a VAT-ID certificate attestation at the Tax Administration on behalf of a Company with an EUDI wallet. The VAT-ID certificate attestation is issued to the EUDI wallet of the VAT-ID certificate holder:



2) The VAT-ID certificate holder requests a VAT-ID certificate attestation at the Tax Administration on behalf of a company with an EUDI Wallet. The address of the Business Wallet, for example through the EBWOID, must be included in the VAT-ID certificate request. This enables the Tax Administration to issue the VAT-ID certificate to Business Wallet of the company.



Flow 3.1b) Retrieval of VAT-ID certificate with authorisation attestation

Goal: a legal representative residing in Country B retrieves VAT-ID certificate attestation at the Tax Administration in Country A on behalf of a company in Country A through Tax Portal where the authorisation is confirmed with an *authorisation attestation*. The VAT-ID certificate is issued to either the EUDI wallet or the Business Wallet of the VAT-ID certificate holder. BU3 supports both flows.

Flow 3b presents an alternative model in which the tax administration requests not only the PID but also a specific authorisation for the intended action directly from the EUDI wallet. In that case, the verification against the authorisation register is not required.

The process assumes that, prior to initiating the request, the authorised person has obtained the necessary authorisation attestation. The process of obtaining an authorisation

attestation is shown in both **Flow b.1 (See Annex 2)**. If using the intermediary, the process of obtaining an authorisation attestation is shown in **Flow b.1a (See Annex 3)**.

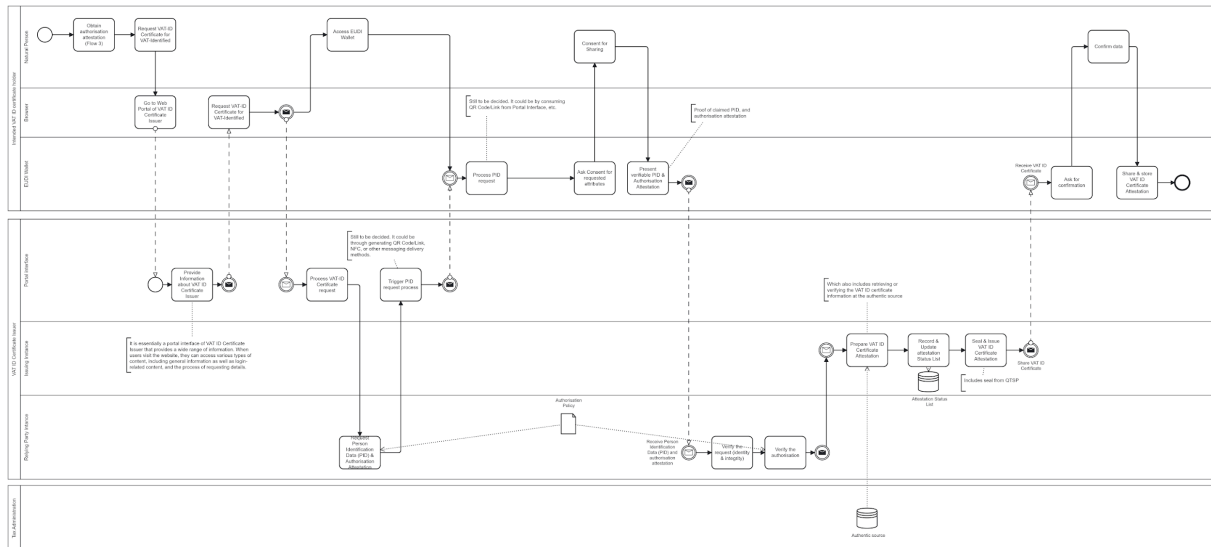
Upon receipt of the VAT ID certificate request and the accompanying authorisation attestation, the Tax Administration performs a number of verification steps in line with its authorisation policy. This includes checking the authorisation attestation issuer, integrity, validity period, and, where applicable, revocation or status information. The Tax Administration must also verify that the attestation is actually relevant to the request being processed and covers the specific action of requesting a VAT ID certificate, or an equivalent/broader scope defined in the applicable policy. Thus, the attestation scope must reference the VAT ID service or broader. Depending on the policy, the Tax Administration may require, for example, that the authorisation evidence be traceable to a person entitled to represent the company with a unlimited PoA or service-based authorisation, that the attestation contain the required representation and assurance attributes (see attestations above), and that all trust anchors and trust service providers involved be acceptable under the Tax Administration's policy framework.

The Tax Administration will only proceed the VAT ID certificate issuance if all technical and authorisation policy checks succeed. The Tax Administration then prepares the attestation, by retrieving information from its sources (in the case of a QTSP, by retrieving or verifying attributes from the sources of the Tax Administration) and issues the VAT ID certificate attestation to either the EUDI wallet or the Business Wallet of the VAT-ID certificate holder.

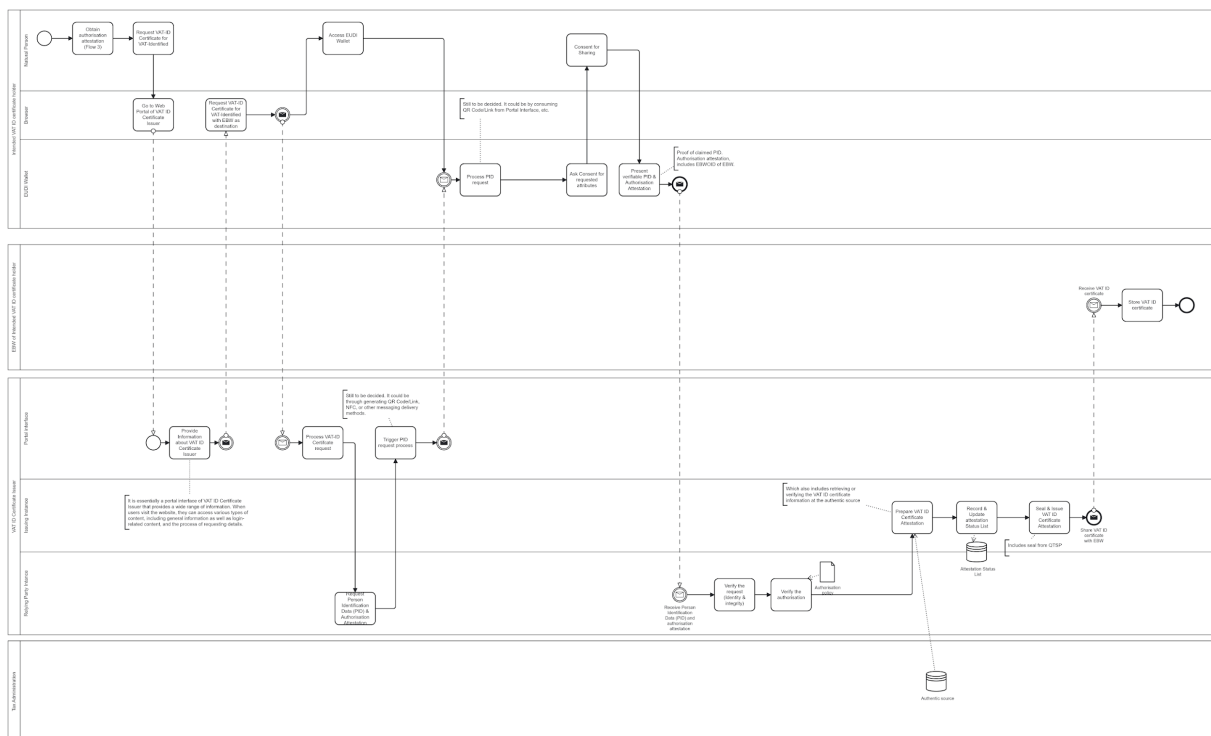
At this stage, there are four main actors with some sub-actors/systems as follows:

- Intended VAT-ID Certificate Holder, which involves the Natural Person and their EUDI Wallet.
- VAT ID Certificate Issuer, which involves Portal Interface, Issuing Instance, Relying Party Instance, and Relying Party Back End.
- Tax Administration as authentic source
- Authorisation Register

1) The VAT-ID certificate holder requests a VAT-ID certificate attestation at the Tax Administration on behalf of a Company with an EUDI wallet. The VAT-ID certificate attestation is issued to the EUDI wallet of the VAT-ID certificate holder:



2) The VAT-ID certificate holder requests a VAT-ID certificate attestation at the Tax Administration on behalf of a company with an EUDI Wallet. The address of the Business Wallet, for example through the EBWOID, must be included in the VAT-ID certificate request. This enables the Tax Administration to issue the VAT-ID certificate to Business Wallet of the company.



2.4 Scenario additional flows

The following table presents an overview of subscenario's and variants supported by BU3 in scenario 1. When we pilot variant 1b, we have specified supporting processes that are called upon by the main flow. We will specify these in the designated annexes.

Flow	Short description
<i>Main flow</i>	<i>Two main alternative authorisation verification patterns for VAT-ID Certificate Retrieval through Tax Portal.</i>
3.1a) Retrieval of VAT-ID Certificate with Authorisation Register	An authorised person requests the VAT ID certificate and indicates whether the certificate must be issued to its EUDI or Business Wallet. The service-based authorisation is verified through a lookup by the National Tax Administration at the central authorisation register. Once it is proven that the authorised natural person has the authorisation to retrieve the VAT ID Certificate, then VAT ID Certificate Issuer will issue the VAT ID Certificate to the EUDI wallet of the authorised person or Business Wallet of the company. BU3 would specifically like to pilot revocation of the authorisation within its use case.
3.1b) Retrieval of VAT-ID Certificate with Authorisation Attestation	An authorised person obtains a service-based authorisation attestation, requests the VAT ID certificate, indicating whether the certificate must be issued to its EUDI or Business Wallet. After verifying the request and the service-based authorisation attestation, the VAT ID Certificate Issuer will issue the VAT ID Certificate to the EUDI wallet of the authorised person or Business Wallet of the company.
<i>Variations</i>	
Issuing instance	The main flows show a generic VAT ID certificate issuer. BU3 would like to pilot with issuing a Pub-EAA and QEAA by verifying or retrieving attributes by the NTA source. These variants can apply to both 3a and 3b and will be specified by the National Tax Administrations in v1.0. BU3 would specifically like to pilot revocation of the authorisation within its use case.
3.2) Retrieval of VAT-ID Certificate with rights based upon a PoA	A fully authorised person obtains a PoA, requests the VAT ID certificate, indicating whether the certificate must be issued to its EUDI or Business Wallet. After verifying the request and the PoA, the VAT ID Certificate Issuer will issue the VAT ID Certificate to the EUDI wallet of the fully authorised person or Business Wallet of the company.
3.3) VAT-ID Certificate Retrieval through an intermediary company in country B based upon PoA	Conceptually, the process is same as Flow 3.1 and 3.2. However, now it is not the person from the VAT identifiable person in country A filing the VAT declaration, but a person from an intermediary in another country B. The authorised person from the Intermediary company requests the VAT ID certificate on behalf of an intermediated company. The authorisation of the natural person is provided with an PoA. The Intermediary must also be authorised, thus the intermediary company has to obtain an authorisation from the intermediated company in country A. This can be done based on the authorisation register (3a), or based on an authorisation attestation (3b). After verifying the request, the VAT ID Certificate Issuer will issue the VAT ID Certificate to the EUDI wallet of the authorised person from the Intermediary or Business Wallet of the Intermediary. BU3 would specifically like to pilot revocation of the authorisation within its use case.
3.4) VAT-ID Certificate Retrieval through an intermediary company in country B with	Conceptually, the process is same as Flow 3.3. The authorised person from the Intermediary company requests the VAT ID certificate on behalf of an intermediated company. The authorisation of the natural person is provided with a service-based authorisation attestation (flow

service-based authorisation within intermediary company.	3b). The Intermediary must also be authorised, thus the intermediary company has to obtain an authorisation from the intermediated company in country A. This can be done based on the authorisation register (3a), or based on an authorisation attestation (3b). After verifying the request, the VAT ID Certificate Issuer will issue the VAT ID Certificate to the EUDI wallet of the authorised person from the Intermediary or Business Wallet of the Intermediary. BU3 would specifically like to pilot revocation of the authorisation within its use case.
<i>Supporting processes</i>	
b.1a The fully authorised/authorised natural person registers at the authorisation register – fully authorised person initiated.	Detailed in Annex 2. This process is when the fully authorised/authorised person is registered in an authorisation register initiated by fully authorised person. This register is later accessed to obtain the authorisation attestation.
b.1b The fully authorised/authorised natural person registers at the authorisation register – person to be authorised initiated	Detailed in Annex 2. This process is when the fully authorised/authorised person is registered in an authorisation register initiated by the to be authorised person. This register is later accessed to obtain the authorisation attestation.
b.2. Retrieval of authorisation attestation at the authorisation register by authorised person.	Detailed in Annex 2. Authorised person obtains the attestation from authorisation register. This attestation is used for filing VAT Declaration for the associated company.
b.3. Retrieval of authorisation attestation by intermediary company.	Detailed in Annex 3. This process is when the VAT-ID Certificate retrieval will be done by the intermediary company. To make it possible, the intermediary company first must obtain authorisation from intermediated company by being registered in the authorisation register of the intermediated company and obtain an authorisation attestation.
Exceptions	NA

2.5 Challenges and barriers

BU3 foresees the following challenges and barriers towards the piloting of scenario 3:

(1.7) Specifications of scenario's are not ready in time for the participants to develop and implement.

(1.7) Specifications of authorisation attestation are not ready in time for the participants to develop and implement.

(new) Specifications of Identity Matching are not ready in time for the participants to develop and implement.

2.6 Working Assumptions

To be specified by National Tax Administrations.

3 Detailed scenario flow

Per step in the main flows, a detailed description is made in the table below.

Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Request VAT-ID Certificate for VAT-identified (Flow 3a, and 3b)	Intended VAT ID Certificate Holder (Natural Person / Browser)	A natural person initiates the request of VAT-ID Certificate for VAT-Identified		An alternative way to prove authorisation is by accessing a central authorisation register (flow 3a).
Access Tax Administration Web Portal (Flow 3a, and 3b)	Intended VAT ID Certificate Holder (Natural Person / Browser)	It marks the start of the process, where a Natural Person accesses the Web Portal of Tax Administration, and starts the request.		
Request and present PID (Flow 3a, and 3b)	NTA (Portal / Relying Party Instance)	Portal triggers a PID presentation request towards the EUDI Wallet. Trigger method (QR code, deeplink, or NFC) is to be determined by each piloting party. In flow 3b, the portal also requests the authorisation attestation obtained by the VAT ID certificate holder.	PID, EBWOID	The address of the Business Wallet, for example through the EBWOID, must be included in the VAT-ID certificate request. This enables the Tax Administration to issue the VAT-ID certificate to Business Wallet of the company.
	Intended VAT ID Certificate Holder (EUDI Wallet / Natural Person)	EUDI Wallet presents a consent screen showing the requested attributes. A natural person approves. Wallet presents the PID and requested attributes to the relying party instance.	PID, EBWOID	
Verify the request (Identity, Integrity, authorisation)	NTA (Backend / Authorisation Register)	Relying Party Instance of Tax Administration verifies the request, which includes verifying identity and integrity.	PID Authorisation Attestation	
		The Tax Administration verifies the service-based authorisation of the natural	Authorisation attestation	In flow 3a, the Tax Administration will check the central

		person in line with its authorisation policy.		authorisation register in line with its authorisation policy. In flow 3b, the Tax Administration will verify the presented authorisation attestation in line with its authorisation policy.
Prepare, seal, and issue VAT-ID Certificate Attestation	NTA (Issuing Instance)	Issuing Instance of Tax Administration prepares VAT-ID Certificate Attestation, which includes retrieving VAT ID Certificate information at the authentic source. Then, issuing instances also record and update attestation status list to the status list. Once it is done, the VAT ID Certificate is sealed and issued to EUDI Wallet/Business Wallet.	VAT-ID Certificate Attestation	There are two ways of storing VAT ID Certificates, either through EUDI Wallet, and Business Wallet.

4 Roles and participants

4.1 Scenario roles and participants

Scenario 3 includes several authentic sources that serve as the basis for the VAT ID certificate: the Tax Administrations from Gipuzkoa, Finland, and Netherlands. The users of EUDI and Business Wallet are mocked. The presentation of the VAT ID certificate is out of scope in BU3, therefore, the relying parties are present in other WE BUILD use cases.

Primary role	UC partner Name	Country
1. User of EUDI & Business Wallet	Mocked	
2. Authentic sources	Tax Administrations for VAT ID: Gipuzkoa Tax Administration Finnish Tax Administration Dutch Tax Administration	GI FI NL
3. Relying party	Relying Parties of VAT ID certificates are not part of the use case. The certificate is presented in other WE BUILD use cases.	
4. Intermediary	Mocked	

4.2 Additional roles and partners

The table provides an overview of the partners involved in BU3. Actual partners may differ in the piloting phase, depending on their availability and additional interested parties.

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	Cleverbase Digidentity KPN Digdir	NL NL NL NO	NW
2. Business Wallet provider	Credenco Ledger Leopard Cleverbase	NL NL NL	BW
3. PID Provider	Digidentity KPN Cleverbase Signicat Digdir DIGG	NL NL NL NO NO SE	NW

4. Trusted list registrar	WP4		
5. QEAA provider	Reconi	NL	NW/BW
	Signicat	NO	
	Digidentity	NL	
	Cleverbase	NL	
6. Pub-EAA provider	Netherlands Tax Administration	NL	NW/BW
7. EAA provider	T.b.d.		
8. QES provider	Cleverbase	NL	NW/BW
	KPN	NL	
	Digidentity	NL	
	Signicat	NO	

4.3 Target country combinations

Scenario 3 involves three countries with authentic sources, which are Tax Administrations; Gipuzkoa, Finland, and the Netherlands. At this stage, the Finnish Tax Administration has confirmed its intention to pilot the scenario with both Gipuzkoa and the Dutch Tax Administration. For Gipuzkoa and the Dutch Tax Administration, discussions regarding their respective pilot partners are still ongoing, and the final country combinations have not yet been confirmed. Consequently, the Holder Country, which is expected to represent the company in Country A, remains to be determined.

Holder country (Representative from company in country A)				
Issuing country (Tax Administration)	Country	GI	FI	NL
	GI			
	FI			
	NL			

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

The following table presents the attestations to be provided by other UCs/WGs/scenarios: which consist of PID, EBW-OID, PoA, and Authorisation Attestation which involves WP2 and WP4 as seen on Table below.

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Person Identification Data (PID) is the core credential issued by Member States that digitally identifies a Natural Person is. It is used to verify Natural Person's identity across EU.	PID provider	Gipuzkoa (Spain), Finland, Netherlands	The PID must contains: 1) The mandatory attributes to identify the natural person based on 2977/2024. 2) The optional attributes needed as additional information to the mandatory attributes, which varies per member state.
EBW-OID	European Business Wallet Organization Identification Data (EBWOID) is the core credential issued by Member States that digitally proves the identity of legal person/company. It acts as digital company ID to be used both for public, and private sector.	EBWOID Provider	Gipuzkoa (Spain), Finland, Netherlands	The EBWOID must contains: 1) The mandatory attributes to identify the company. 2) The optional attributes needed as additional information to the mandatory attributes, which varies per member state.
PoA	Power of Attorney (PoA) is an authorisation only owned by Authorised Persons to act on behalf of a specific company, with larger scope of authorisation.	BU4	Gipuzkoa (Spain), Finland, Netherlands	Defined by BU4.
Authorisation attestation	Authorisation attestation is an attestation that proves natural/legal person could act on behalf of other natural/legal person.	BU4	Gipuzkoa (Spain), Finland, Netherlands	Authorisation attestation must include the service-based scope defined by the TA

5.3 Created attestations in the scenario

There is one attestation created in this scenario: a VAT-ID Certificate Attestation.

Attestation name	Short description	From Countries	Applicable domain standards
VAT ID certificate	VAT ID Certificate is an attestation stored in EUDI Wallet/Business Walle issued by Tax Administration confirming that a company is registered for VAT.	Gipuzkoa (Spain), Netherlands, Finland	VAT ID Certificate must contain attributes defined in the draft of VAT ID Certificate Rulebook (See: https://portal.webuildconsortium.eu/group/5/files/9363/collaboration/online/edit/4928)

Annex 1 – Requirements for scenario roles

This annex lists the main functional/ organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
User of EUDI Wallet	a. BU3 partners will mock users b. Must possess a valid EUDI Wallet containing at least a PID and, depending on the sub-scenario optionally an authorisation attestation (service-based) or a Power of Attorney (PoA).
Authentic source	a. Must provide authoritative, accurate, and current information regarding VAT ID. b. Non-specific for BU3 - Must offer secure interface that enable verification and validation processes. c. Non-specific for BU3 - Must provide mechanisms to communicate or expose status updates, including revocations or other relevant changes.
Relying party	a. Relying Parties of VAT ID certificates are not part of the use case. The certificate is presented in other WE BUILD use cases. b. The VAT ID must be able to be issued to both an EUDI wallet and Business wallet
Business Wallet Provider	a. Must hold a Business Wallet containing EBWID and must have obtained a valid authorisation from the intermediated company in Country A (either via central authorisation register (3a) or authorisation attestation (3b)) before a natural person from the intermediary can request a VAT ID certificate on the intermediated company's behalf. b. Non-specific for BU3. Must support an authorisation register as specified in the Business Wallet regulation. c. Must support authorisation attestations – both for employees and for representing other organisations in flows for 1b.
EUDI Wallet Provider	a. Non-specific for BU3 - Must enable OpenID4VP interactions b. Non-specific for BU3 - Must verify credentials for integrity, authenticity, trust status, and revocation status c. Non-specific for BU3 - Must integrate with trusted lists and credential validation services d. Non-specific for BU3 - Must already contain authorisation attestation, and PID before the transaction process begins.
PID Provider	a. Must issue PID containing both mandatory, and optional attributes based on Member States. Each Tax Administration defines the identity data required for scenario 1. b. Non-specific for BU3 - Must support secure PID issuance, renewal, and revocation c. Non-specific for BU3 - Must provide up-to-date status information for trust and revocation need.
Trusted list registrar	a. Non-specific for BU3 - Must maintain and publish trusted lists b. Non-specific for BU3 - Must ensure trust status information is available and accessible for validation purposes. c. Non-specific for BU3 - Must provide machine-readable interfaces for trusted list access and consumption.
QEAA provider	d. Non-specific for BU3 – Tax Administrations piloting with QEAA must comply with generic QEAA requirements. e. Tax Administration is used as authentic source
Pub-EAA provider	a. Non-specific for BU3 – Tax Administrations piloting Pub-EAA must comply with generic Pub-EAA requirements.

	b.	Tax Administration is used as authentic source
EAA provider	a.	Non-specific for BU3.
QES provider	b.	Non-specific for BU3 - QES must be supported to submit VAT ID certificate request
	c.	Non-specific for BU3 – Tax Administrations must be able to seal VAT ID certificate.

Annex 2 – Authorisation Registration and Attestation Retrieval Flows

Flow 3.1b.1a & 3.1b.1b: Entering and accepting an authorisation in a trusted authorisation register

Right after retrieving the PoA attestation, a fully authorised natural person uses an EUDI Wallet to demonstrate their authority and update the organisation's authorisations.

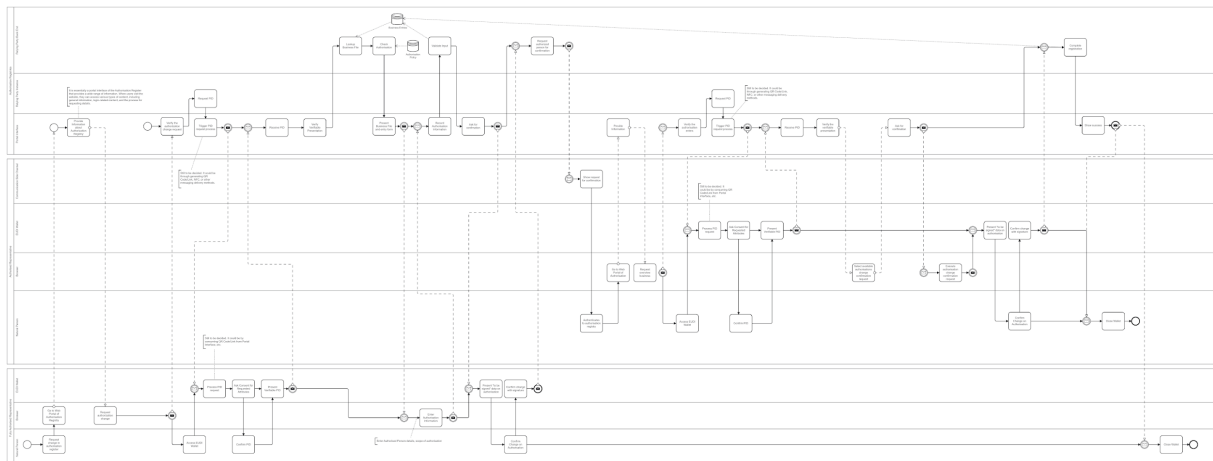
Three aspects are key. First, a generic register is used, which determines through an authorisation policy that the person is allowed to manage authorisations. Second, authorisation categories are not yet specified. For the BU3 use case, these would need to align with those used by the VAT ID certificate issuer, but here they remain generic. Third, the update is confirmed with a qualified electronic signature via the wallet. While not always required, this adds non-repudiation and is especially valuable if the register serves external purposes, such as within a business wallet, where it can support issuing attestations.

In system-to-system interactions, entries may instead be authenticated using a qualified electronic seal. If the register is part of a business wallet or operated by a trusted third party, it may also include authorisations for individuals who can manage it for specific services. This enables a layered, hierarchical authorisation model.

There are **two ways** of putting an entry to the authorisation register, such as:

- **b.1a)** Fully authorised person registers authorisation, and authorised person accepts
- **b.1b)** Person to be authorised registers authorisation, and fully authorised person accepts

Flow b.1a) fully authorised person registers authorisation, authorised person "accepts"

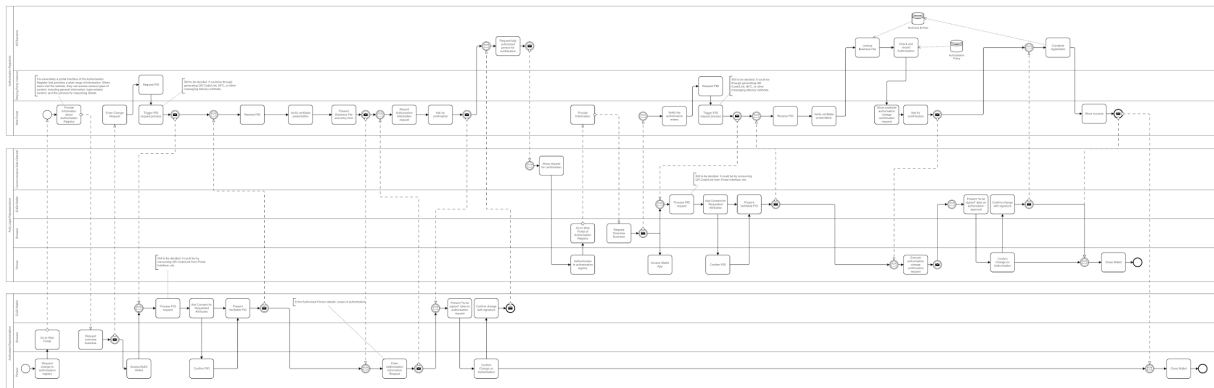


This is the first way of natural person putting an entry to the authorisation registry regarding the authorisation. This way is possible when the fully authorised person wants person to be authorised to do the process on their behalf.

In this process, there are three main actors involved, such as:

- Fully Authorised Representative, which involves Natural Person, and EUDI Wallet
- Authorised person, which involves Natural Person, and EUDI Wallet
- Authorisation Registry, which involves Portal Interface, Relying Party Instance, and Relying Party Back End

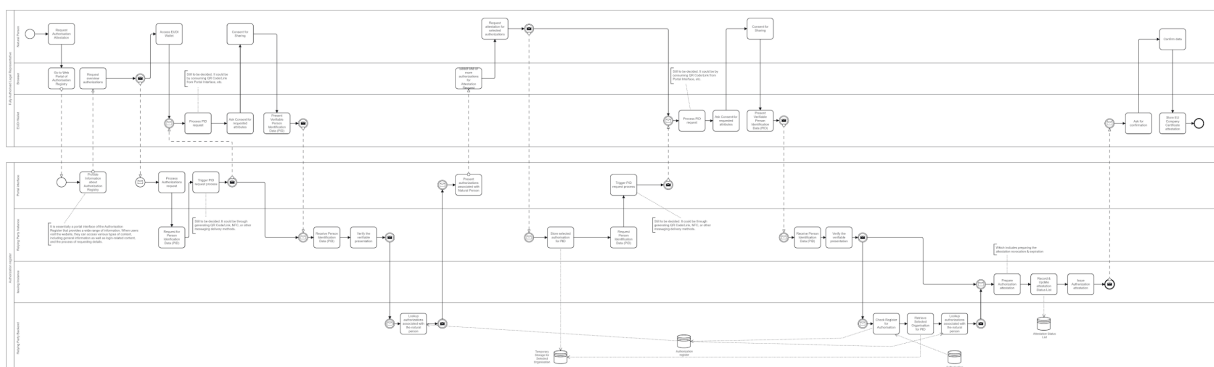
Flow b.1b) person to be authorised registers authorisation and fully authorised person accepts.



This process is the other option for the authorised person to obtain the authorisation from the fully authorised person. However, for this way, instead of fully authorised person giving authorisation to authorised person, the authorised person requests for that authorisation to the fully authorised person.

The main and sub-actors involved are same as those involved in 1.1b.1a process.

Flow b.2: Retrieval of authorisation attestation at the authorisation registry



This flow is executed to retrieve an authorisation attestation necessary for **Flow 3.1b, 3.3b, 3.4b**. In these flows, we use an authorisation attestation as proof of authorisation to obtain a VAT-ID certificate. The idea is that the fully authorised person obtains the authorisation attestation at the authorisation registry. This registry can have multiple forms, for example, it can be kept by a Tax Administration, but it could be a Business Wallet. The (fully) authorised person authenticates himself to the authorisation registry using their PID, the authorisation registry does the lookup to their system to check on the available

authorisations, the (fully) authorised person selects the authorisation for attestation issuance, and the authorisation registry prepares the authorisation attestations.

For this process, there are two main actors involved such as:

- The fully authorised representatives, which involves Natural Person, and EUDI Wallet.
- The Authorisation Registry, which involves Web Portal/Portal Interface, Relying Party Instance, Issuing Instance, and Authorisation Registry Backend.

Annex 3 – Authorisation Registration and Attestation Retrieval Flows of Intermediary Company

Flow b.3: Retrieval of authorisation attestation by intermediary at the authorisation register

In Flow 3b.1, we also discuss about retrieving an authorisation attestation. However, that authorisation attestation is only available for the authorised natural person working at the same company as the fully authorised natural person. It is like a boss asking for his employee

to do something for him. However, in some occasions like tenders, the intermediary company needs the VAT ID certificate of the intermediated company.

This process is the same in every scenario of BU3.

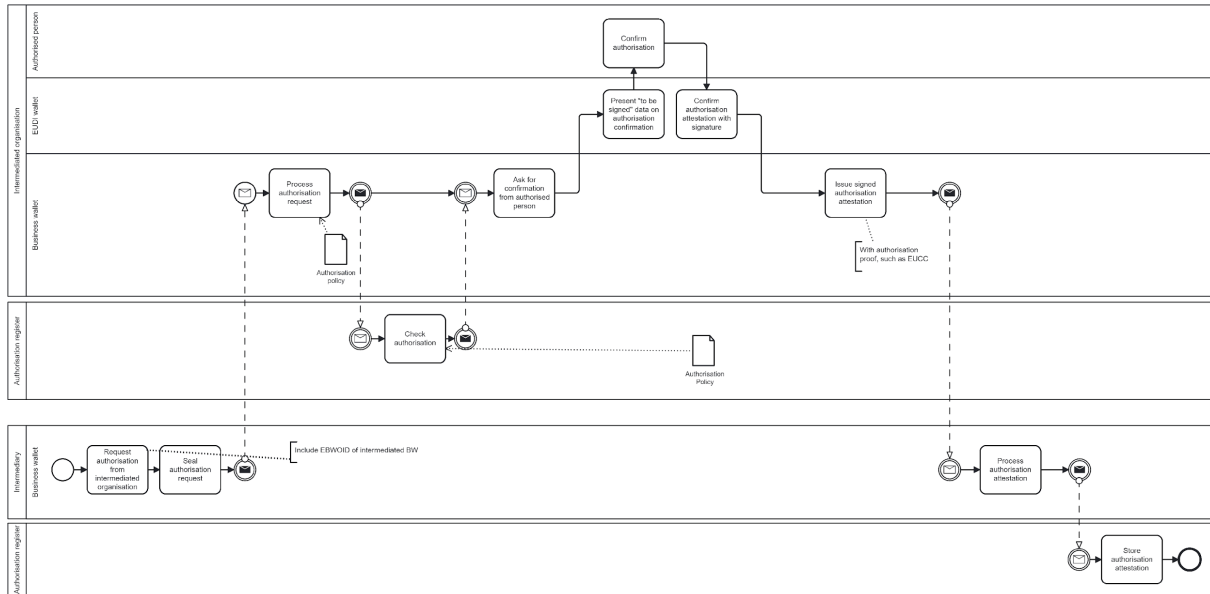
The process establishes an authorisation attestation for later use by the intermediary. The intermediary business wallet sends a sealed request to the intermediated organisation, the business wallet of the intermediated company verifies the request by accessing its authorisation register, obtains confirmation from an authorised person via the EUDI wallet, records the authorisation, and issues a signed or sealed authorisation attestation. The issued attestation is then sent back to the intermediary business wallet and stored in an authorisation register.

A prerequisite for this process is that the intermediary is registered in the authorisation register of the intermediary process. This process is explained in scenario 1 for natural persons and can be re-used for registering intermediaries.

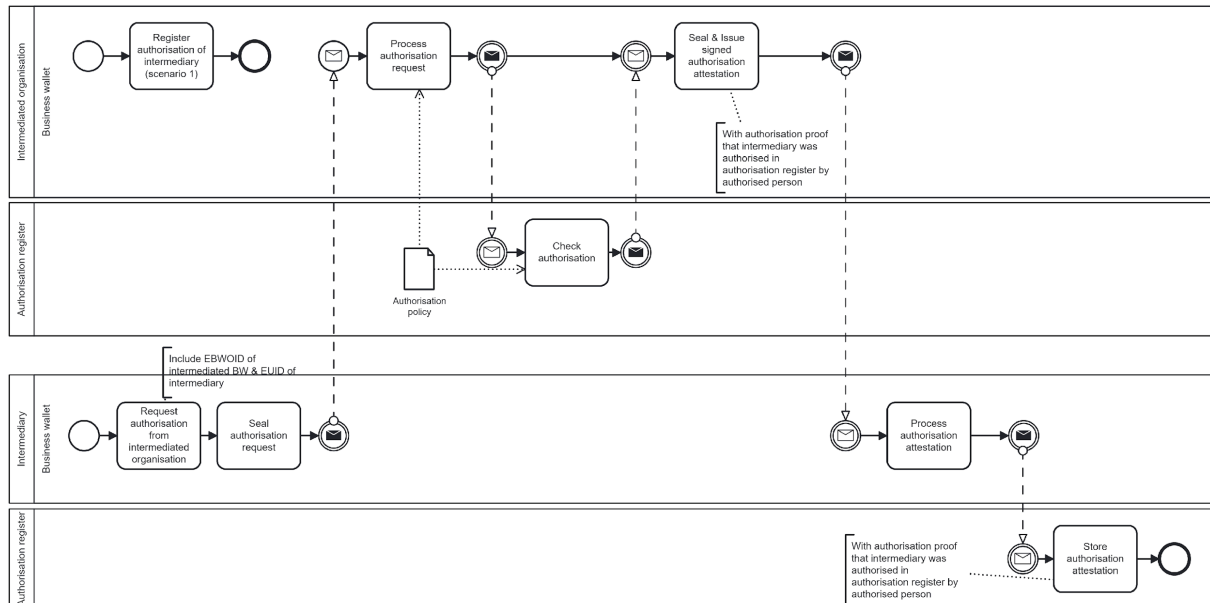
While this is not always required, the capability of an EUDI wallet makes this a highly relevant perspective. It introduces non-repudiation, which becomes particularly valuable if the register serves an external function, for example as part of a business wallet, where it can also provide a foundation for issuing attestations based on the register. This effectively turns it into a generic function that can be reused within the business wallet (**subscenario b.3a**). In full system-to-system interactions, an entry may alternatively be considered authentic when it is sealed with a qualified electronic seal (**subscenario b.3b**).

It is therefore important to note that this register, if it becomes part of a business wallet or is operated by an external trusted party, may also contain the proof or authorisation information regarding individuals who are permitted to manage and modify the register for specific services, such as authorisation of intermediaries in their authorisation register. This way, the chain of authorisation in authorisation attestations issued to intermediaries and applied in VAT declaration or VAT ID certificate issuance processed, can be validated by the Relying Party of Issuer. This enables a layered or hierarchical authorisation model.

b.3a - Issuance of authorisation attestation with Qualified Electronic Signature



b.3b - Issuance of authorisation attestation with Qseal

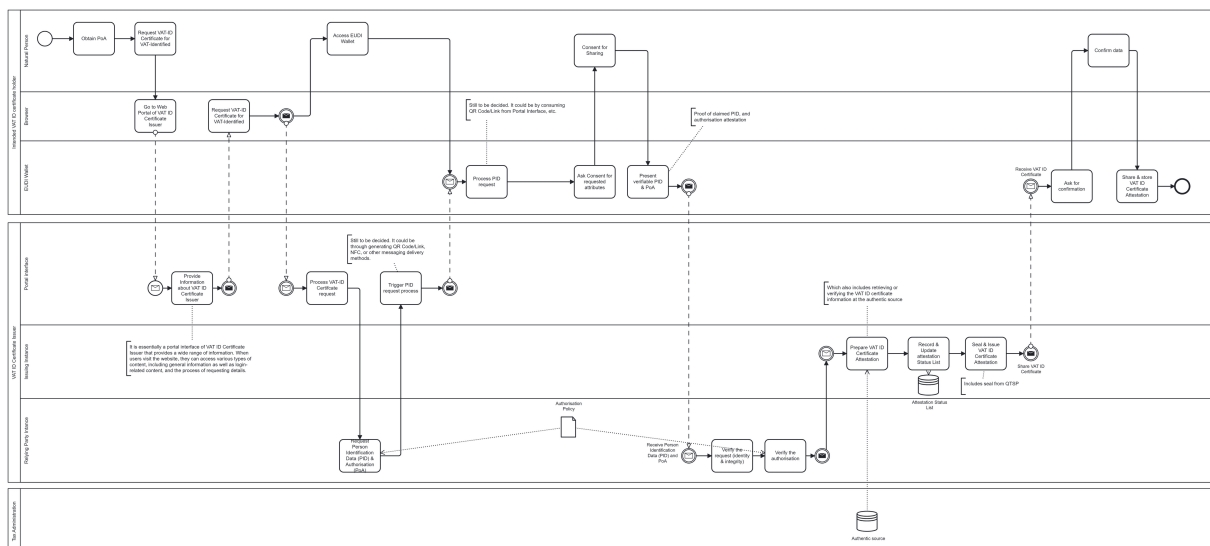


Annex 4 – Retrieval of VAT-ID Certificate with rights based upon a PoA

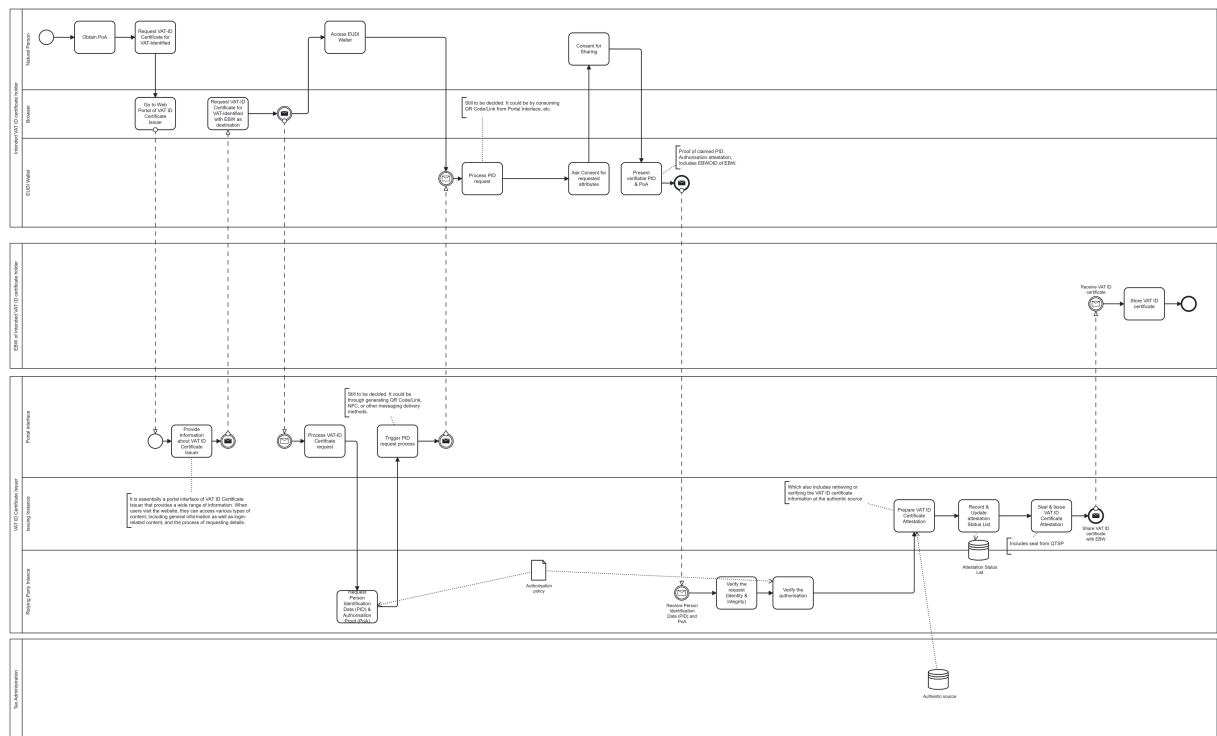
Flow 3.2) Retrieval of Vat-ID certificate for EUDI wallet by authorised person based on PoA

A person who is authorised to act as the holder of a VAT-ID certificate, the Authorised Person, obtains a PoA and presents himself at the tax administration portal using their EUDI wallet and their PoA attestation. The portal uses a relying party instance to have the person identify themselves with their PID. Based on the PID and the PoA, the tax authority can verify whether the person is authorised to act as the holder of the VAT-ID certificate for the specified VAT-identified taxable person. Once confirmed, the certificate can be issued to the EUDI wallet of the authorised person or the Business Wallet of the company.

1) The Authorised Person with a PoA requests a VAT-ID certificate attestation at the Tax Administration on behalf of a Company with an EUDI wallet. The VAT-ID certificate attestation is issued to the EUDI wallet of the VAT-ID certificate holder:



2) The Authorised Person with a PoA requests a VAT-ID certificate attestation at the Tax Administration on behalf of a company with an EUDI Wallet. The address of the Business Wallet, for example through the EBWID, must be included in the VAT-ID certificate request. This enables the Tax Administration to issue the VAT-ID certificate to Business Wallet of the company.



WE BUILD consortium

Specification

Scenario 4 - Issuing

VAT-ID Using M2M

WP2 – VAT-ID Certificate Issuance Using M2M Interaction

Date : June 22th , 2026
Version : 1.0
Status : Final

Index

1 Introduction3

1.1 Objectives of this document3

1.2 Scenario introduction3

2 Scenario specification4

2.1 Introduction: Issuing VAT ID using M2M4

2.2 Scenario pre-conditions5

2.3 Scenario main flow5

8

9

9

3 Detailed scenario flow10

4 Roles and participants12

4.1 Scenario roles and participants12

4.2 Additional roles and partners12

4.3 Target country combinations12

4.4 Requirements13

5 Attestations14

5.1 Introduction14

5.2 Attestations to be provided by other UCs/WGs/scenarios14

5.3 Created attestations in the scenario15

16

16

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 4, as part of use case Foreign Tax Declaration (BU3) in work package 2 in the WE BUILD consortium. This version constitutes the generic specifications of this BU3 scenario, and is supported by the specification documents of National Tax Administrations part of this scenario. The generic specifications explain the piloted flows by BU3 in general. However, tax processes are characterised by their national context. Therefore, the participating National Tax Administrations have defined the variants of the flow they will pilot and possible deviations from the generic flow in their specification documents.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

In short, the objective of Scenario 4 is that a business wallet of an intermediary company in Country B requests and receives a VAT ID certificate as an attestation from a Tax Administration in Country A on behalf of a Company from Country A as a M2M interaction. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved. The final chapter explains what will be learned from the scenario. The final chapter explains what will be learned from the scenario.

The scenario is based on the following documentation:

- Stock Taking Document
- BPMNs
- Architecture Reference Framework (ARF) V2.9
- We Build Architecture & Integration Blueprint
- We Build Attestation Rulebooks Catalogue

2 Scenario specification

2.1 Introduction: Issuing VAT ID using M2M

In short, scenario 4 concerns a business wallet of an intermediary company in Country B that requests a VAT ID certificate as an attestation from Tax Administration in Country A on behalf of a Company from Country A. This scenario is part of the MVP and will primarily use a Business Wallet, possibly an EUDI wallet to confirm authorisations. The identity of the intermediary company is guaranteed by a qualified electronic seal on the VAT ID request. The identity of the natural person involved is guaranteed by a qualified electronic signature, if required by law for a required level of assurance on approval.

Similar to scenario 1-3, scenario 4 pilots the authorisation of the intermediary in two ways:

- **Scenario 4a:** Checking a central register – in this document referred to as an authorisation register.
- **Scenario 4b:** Proof of Authorisation – in this document referred to as an authorisation attestation; and/or,

The National Tax Administration in BU3 decide whether they will pilot scenario 4a and/or 4b. This will be specified in version 1.0 by each National Tax Administration.

The following table shows the flows part of scenario 4:

Flow	4a. Authorisation attestation	4b. Authorisation register
4a. Obtaining a VAT ID with authorisation register		X
4b. Obtaining a VAT ID with authorisation attestation	X	
4b-1. Obtaining an authorisation attestation (Annex 2)	X	

The VAT ID certificate attestation is issued either as a Qualified Electronic Attestation of Attributes (QEAA) or as a Public Sector Body Electronic Attestation of Attributes (PUB-EAA), and is in other use cases presented to a relying party seeking a high level of assurance regarding the authenticity, integrity, and validity of the VAT identification number. What model each National Tax Administrations will pilot is specified in version 1.0.

The attestation contains the EUID to which the VAT ID number is assigned, as well as the VAT identification number itself.

Attestations to use

- Person Identification Data (PID)
- European Business Wallet Organization Identification Data (EBWOID)
- Service-based authorisation attestation
- Value Added Tax (VAT) ID Certificate Attestation

2.2 Scenario pre-conditions

The following specific prerequisites exist for the use case and its scenarios:

- All natural persons involved (acting on behalf of a company or an intermediary organisation) have an EUDI Wallet containing PID.
- All organisations involved have an EUID and a business wallet containing EBWOID.
- There are one or more attestations that covers “acting on behalf of a legal person” defined.
- Where applicable, there is an authorisation mechanism in place to consult a central authorisation to verify the authorisation of the Intermediary. This is out of scope for WE BUILD.

2.3 Scenario main flow

The main objective of scenario 4 is to model a scenario where an intermediary in Country B wants to retrieve VAT ID Certificate at the Tax Administration in Country A on behalf of a company in Country A through Machine to Machine (M2M) with a business wallet. Scenario 4 has two main flows: issuing a VAT ID certificate attestation based on 4a) an a central authorisation register and based on 4b) an authorisation attestation. Both flows set out the process by which an intermediary Business Wallet (BW) obtains a VAT ID certificate on behalf of an intermediated company.

In both flows, the actor issuing the VAT ID certificate is referred to as the “VAT ID Certificate Issuer”. This is a general term used to cover different issuing models. The VAT ID certificate can be issued either as a Pub-EAA (Public Electronic Attestation of Attributes) or as a QEAA (Qualified Electronic Attestation of Attributes). A Pub-EAA is issued by the Tax Administration with a qualified electronic seal, while a QEAA is issued by a Qualified Trust Service Provider (QTSP) that retrieves or verifies the attributes at the Tax Administration source. The applicable issuing model depends the pilot goals of the National Tax Administrations in BU3.

Both flows begin when the Intermediary BW creates a VAT ID certificate request and sends it to a specific VAT ID Certificate Issuer for this use with their (technical) address. The VAT ID Certificate Issuer will either use a BW or their own specified digital environment. When the national Tax Administration pilots with a BW, the request could include the EBWOID of the Tax Administration BW so that the request can be addressed and routed to the intended recipient wallet. The address should include a specification to a specified Tax Administration BW to account for the scenario where one Relying Party has multiple BWs. The Intermediary BW includes its own identification (EBWOID) and the identification of the intermediated company.

In general, the following requirements apply:

- The Intermediary BW can send a VAT ID certificate request to a specified VAT ID Certificate Issuer.
- The VAT ID Certificate Issuer can verify that the request originates from the intermediary legal entity (e.g. via Qualified Electronic Seal, EBWOID).
- The VAT ID Certificate Issuer can verify that the intermediary is authorised to act on behalf of the intermediated company. In Scenario 4a is done via a central

authorisation attestation, while 4b this is done via an authorisation attestation. The intermediated company must be clearly identified to process the request.

- We have not specified the authorisation register used for the authorisation attestation. This authorisation register may operate within the BW or by a trusted third party such as a QTSP.

Interaction between Intermediary Business Wallet and Tax Administration

The flow descriptions intentionally abstract from the full mechanics of establishing trust between systems. In practice, the communication setup may involve mutual authentication, certificate validation, and challenge-response steps that are not explicitly modelled here. The present BPMN focuses on the business messages specific to Scenario 4, rather than on the complete trust protocol.

Accordingly, before processing the request, the VAT ID certificate issuer/Tax Administration authenticates the Intermediary BW as a trusted communication peer. Following the WeBuild architecture, OpenID protocols is be used for issuing and using the VAT-ID certificate and eTRC attestations in BU3 in M2M interactions following the WeBuild architecture. QERDS is used for exchanging documents and notifications in BU3 in M2M interactions, specifically scenario 2 VAT declaration filing, following the WeBuild architecture. Any deviations from the WeBuild architecture by National Tax Administrations are reported in their respective scenario specifications.

Process VAT ID certificate request

Upon receipt of the VAT ID certificate request, the Tax Administration performs a number of verification steps in line with its authorisation policy. The authorisation policy should be defined by the National Tax Administrations in the v1.0 of this document. In addition, when National Tax Administrations pilot with QTSPs issuing QEAAAs, it should be specified who should provide/collect what evidence to prepare the issuance of the VAT ID certificate QEAA.

Issue VAT ID certificate attestation

The Tax Administration will only proceed the VAT ID certificate issuance if all validation and policy checks succeed. The Tax Administration then prepares the attestation, by retrieving information from its sources (in the case of a QTSP, by retrieving information or confirmation from the sources of the Tax Administration) and issues the VAT ID certificate attestation. Finally, the issued VAT ID certificate attestation is transmitted to the Intermediary BW, which receives and stores it for subsequent use.

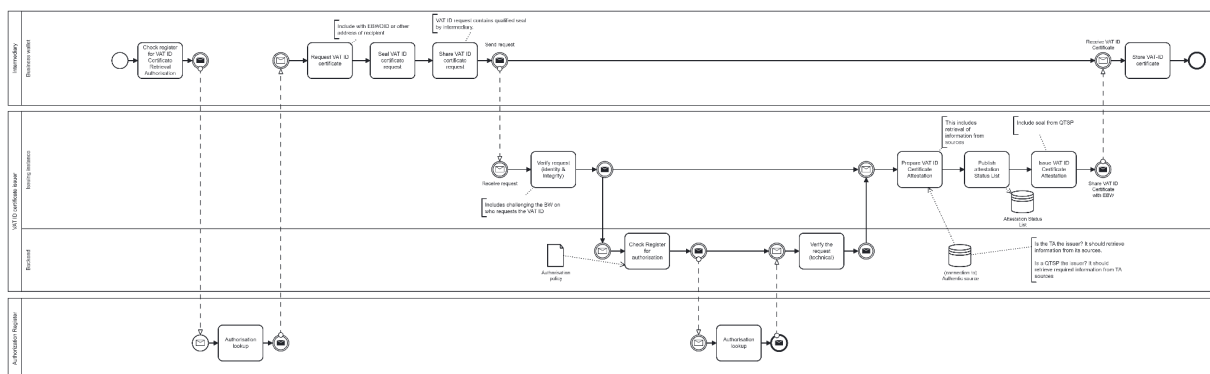
Scenario 4a) Issuing VAT ID using M2M with authorisation register

Goal: an intermediary BW residing in Country B retrieves a VAT-ID certificate attestation at the Tax Administration in Country A on behalf of a company in Country A through M2M where the authorisation is confirmed with a central authorisation register. The VAT-ID certificate is issued to the Business Wallet of the VAT-ID certificate holder. BU3 supports both flows presented below.

In Scenario 4a, the Intermediary BW requests a VAT ID certificate and the VAT ID certificate issuer verifies the authorisation of an intermediary by accessing a central authorisation

register. The main difference compared to Scenario 4b is that the authorisation is not provided in the request itself, but is checked externally through a central authorisation register.

The VAT ID Certificate Issuer consults a central authorisation register to verify whether the intermediary is allowed to act on behalf of the intermediated company. The central authorisation register provides information on whether an authorisation exists, its scope (including whether it covers VAT ID certificate requests), and whether it is still valid or has been revoked. Based on those records, the issuer determines whether the intermediary is authorised to make the request. This flow presumes the existence of a central authorisation mechanism.



Scenario 4b) Issuing VAT ID using M2M with authorisation attestation

Goal: an intermediary BW residing in Country B retrieves VAT-ID certificate attestation at the Tax Administration in Country A on behalf of a company in Country A through M2M where the authorisation is confirmed with an *authorisation attestation*. The VAT-ID certificate is issued to either the EUDI wallet or the Business Wallet of the VAT-ID certificate holder. BU3 supports both flows.

Scenario 4b sets out the process by which an intermediary BW obtains a VAT ID certificate from the Tax Administration on behalf of an intermediated company with an authorisation attestation. This flow assumes that, prior to initiating the request, the intermediary has obtained the necessary authorisation attestation through a separate process detailed in Annex 2.

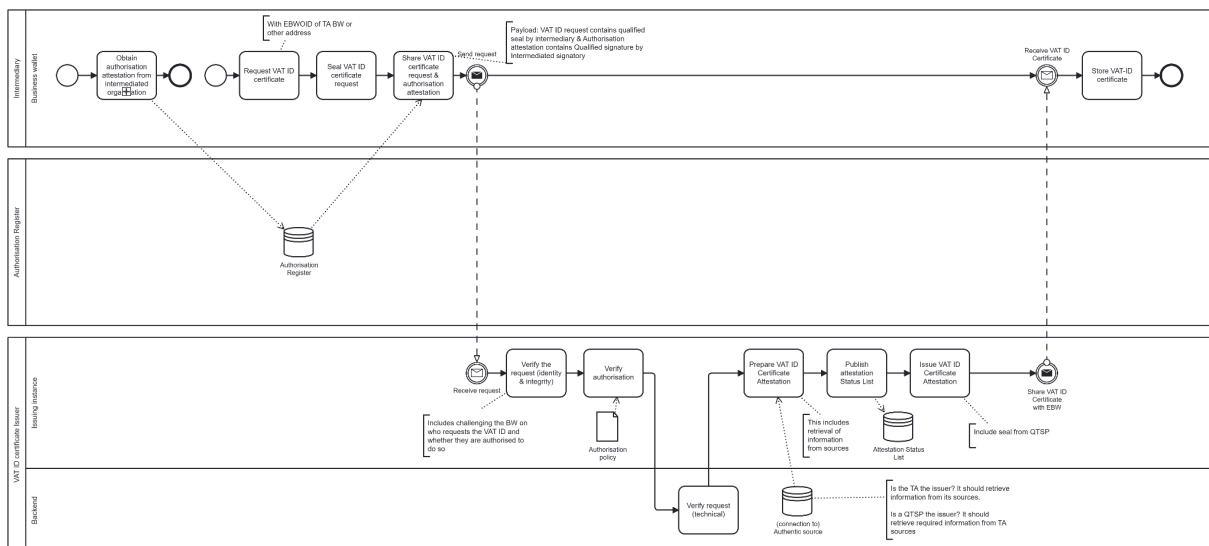
To meet the requirement that the Tax Administration is able to verify that the Intermediary was authorised to make the request on behalf of the intermediated company, the Intermediary BW also presents the authorisation attestation on which it relies. Thus, the Intermediary BW thus includes its own identification (EBW/OID and EUID), the VAT ID certificate request, and the authorisation attestation and identification of intermediated company (EUID) in the same message.

To this end, the Intermediary BW provides the following attestations:

- The EBW-OID of the Intermediary, including the EUID.

- The service-based authorisation attestation (defined by BU4)

Upon receipt of the VAT ID certificate request and the accompanying authorisation attestation, the Tax Administration performs a number of verification steps in line with its authorisation policy. This includes checking the authorisation attestation issuer, integrity, validity period, and, where applicable, revocation or status information. The Tax Administration must also verify that the attestation is actually relevant to the request being processed, i.e. that it binds the identified intermediary to the intermediated company and covers the specific action of requesting a VAT ID certificate, or an equivalent scope defined in the applicable policy. Thus, the attestation scope must reference the VAT ID service or broader. Depending on the policy, the Tax Administration may require, for example, that the authorisation evidence be traceable to a person entitled to represent the company with an PoA, that the attestation contain the required representation and assurance attributes (see attestations above), and that all trust anchors and trust service providers involved be acceptable under the Tax Administration's policy framework.



2.5 Scenario additional flows

The following table presents the main flows and variants piloted in scenario 4.

Flow	Short description
<i>Main flow</i>	<i>Two main alternative authorisation verification patterns for M2M VAT ID certificate retrieval.</i>
-4a. M2M Obtaining a VAT ID with authorisation register	Intermediary BW requests the VAT ID certificate on behalf of a intermediated company without presenting an attestation in the filing. The intermediary and the Tax Administration verifies the authorisation against the central authorisation register.
-4b. M2M Obtaining a VAT ID with authorisation attestation	Intermediary BW requests the VAT ID certificate on behalf of a intermediated company and presents a valid authorisation attestation. The Tax Administration validates the request before processing and issuing the VAT ID certificate to the Intermediary BW.
<i>Variations</i>	
- Issuing instance	The main flows show a generic VAT ID certificate issuer. BU3 would like to pilot with issuing a Pub-EAA or QTSPs issuing a QEAA by verifying or retrieving the attributes at the source.

	These variants can apply to both 4a and 4b and will be specified by the National Tax Administrations in v1.0.
- 4b Obtaining an authorisation attestation	Detailed in Annex 2. The intermediary BW requests an authorisation attestation from the intermediated company, either sealed by the intermediated company or with the intervention of an authorised natural person that signs the authorisation attestation through their EUDI Wallet.
Exceptions	NA

2.5 Challenges and barriers

BU3 foresees the following challenges and barriers towards the piloting of scenario 4:

- (1.7) Specifications of scenario's are not ready in time for the participants to develop and implement
- (1.7) Specifications of Authorisation attestation are not ready in time for the participants to develop and implement
- (1.7) Specifications of M2M-interaction are not ready in time for the participants to develop and implement
- (new) Specifications of Identity Matching are not ready in time for the participants to develop and implement
- (new) Specifications for Interaction between BWs and other actors are not ready in time for the participants to develop and implement

2.6 Working Assumptions

To be specified by National Tax Administrations

3 Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Obtain authorisation attestation from intermediated company (4b)	Intermediary	Flow 4b-1&2, detailed in Annex 2.	Intermediary and Intermediated companies have a BW with EBWID and the intermediated company has registered the authorisation in their authorisation register.	Alternative way to proof authorisation is by accessing a central authorisation register (4a). This happens at the Tax Administration.
Request VAT ID certificate (4a/4b)	Intermediary	To initiate the interaction, the Intermediary BW prepares a VAT ID certificate request addressed to the Tax Administration/VAT ID certificate issuer.	NA	TA may have a BW to process this request.
		VAT ID request is sealed by intermediary BW	NA	
		Intermediary shares VAT ID certificate request and where applicable (4a) the authorisation attestation with Tax Administration	Authorisation attestation EBWID	When using a central authorisation register (4a), only the VAT ID certificate request is shared.
Receive & verify VAT ID certificate request (4a/4b)	National Tax Administration/VAT ID certificate issuer	Upon receipt of the VAT ID certificate request and the accompanying authorisation attestation, the Tax Administration performs a number of verification steps in line with its authorisation policy. This includes checking the authorisation attestation issuer, integrity, validity period, and, where applicable, revocation or status information. It also verifies that the attestation is actually		When using a central authorisation register (4a), the National Tax Administration consults the central authorisation register to verify the request.

		relevant to the request being processed.		
Issue VAT ID certificate	National Tax Administration/VAT ID certificate issuer	The Tax Administration then prepares and issues the VAT ID certificate attestation. Finally, the issued VAT ID certificate attestation is shared with the Intermediary BW.	VAT ID certificate	QEAA Pub-EAA Attribute verification for QEAA. t.b.d by National Tax Administrations in v1.0.

4 Roles and participants

4.1 Scenario roles and participants

Scenario 4 includes two authentic sources that serve as the basis for the VAT ID certificate: the Tax Administrations from Netherlands, and Norway. The presentation of the VAT ID certificate is out of scope in BU3, therefore, the relying parties are present in other WE BUILD use cases.

Primary role	UC partner Name	Country
1. User of EUDI Wallet	Mocked, where applicable.	NO
2. Authentic sources	Tax Administration: Dutch Tax Administration Norwegian Tax Administration	NL, NO
3. Relying party	Relying parties in scenario 4 are from other use cases in We Build.	
4. Intermediary	Mocked	

4.2 Additional roles and partners

The table provides an overview of the partners involved in BU3. It could be that the actual partners differ in the piloting phase, depending on their availability.

Primary role	UC partner Name	Country	Wallet
1. Wallet provider	Cleverbase Digidentity KPN Ubiqu Credenco	NL	NW BW
2. PID Provider			
3. Trusted list registrar	WP4		
4. QEAA provider	Cleverbase, Signicat		BW
5. Pub-EAA provider	Netherlands Tax Administration	NL	BW
6. EAA provider			
7. QES provider	Cleverbase Signicat	NL	NW

4.3 Target country combinations

Scenario 4 involves two countries with authentic sources, which are Tax Administrations; Netherlands, and Norway. At this stage, discussions are still ongoing among Netherlands, and Norway regarding the respective pilot pairings, and no final agreements have been confirmed yet. As a result, the Holder Country, which is expected to represent the company in Country A, has not yet been determined and remains an open point.

	Holder country (Representative from company in country A)		
Issuing country (Tax Administration)		NL	NO
	NL		
	NO		

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

There are two attestations to be provided by other UCs/WGs/scenarios, which consist of service-based authorisation which involves WP2 and WP4 as seen on Table below.

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Person Identification Data (PID) is the core credential issued by Member States that digitally identifies a Natural Person is. It is used to verify Natural Person's identity across EU.	PID provider	Norway	The PID must contains: 1) The mandatory attributes to identify the natural person based on 2977/2024. 2) The optional attributes needed as additional information to the mandatory attributes, which varies per member state.
EBW-OID	European Business Wallet Organization Identification Data (EBWOID) is the core credential issued by Member States that digitally proves the identity of legal person/company. It acts as digital company ID to be used both for public, and private sector.	EBWOID Provider	Netherlands, and Norway	The EBWOID must contains: 1) The mandatory attributes to identify the company. 2) The optional attributes needed as additional information to the mandatory attributes, which varies per member state.
PoA	Power of Attorney (PoA) is an authorisation owned by fully authorised natural/legal person to act on behalf of a specific company.	BU4	Netherlands, and Norway	Defined by BU4. Possibly only in tax portal scenario's.
Service-based authorisation attestation	Authorisation attestation is an attestation that proves natural/legal person could act on behalf of other natural/legal person for a certain service-based scope.	BU4	Netherlands, and Norway	Authorisation attestation must include the service-based scope defined by the TA

5.3 Created attestations in the scenario

There is one attestation created in this scenario, which is a VAT-ID Certificate Attestation, as seen on Table below.

Attestation name	Short description	For Countries	Applicable domain standards
VAT ID certificate	VAT ID Certificate is an attestation stored in EUDI Wallet/Business Wallet issued by Tax Administration confirming that a company is registered for VAT.	Netherlands, and Norway	VAT ID Certificate must contain attributes defined in the draft of VAT ID Certificate Rulebook (See: https://portal.webuildconsortium.eu/group/5/files/9363/collaboration/online/edit/4928)

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
User of EUDI Wallet	a. The BU3 partners will take care for the users
Authentic sources	a. Must provide authoritative, accurate, and current information regarding VAT ID.
	b. Non-specific for BU3 - Must offer secure interface that enable verification and validation processes.
	c. Non-specific for BU3 - Must provide mechanisms to communicate or expose status updates, including revocations or other relevant changes.
Relying party	a. Relying Parties of VAT ID certificates are not part of the use case. The certificate is presented in other WE BUILD use cases.
	b. The VAT ID must be able to be issued to both an EUDI wallet and Business wallet
Intermediary (Business Wallet Provider)	a. Must hold a Business Wallet containing EBWID and must have obtained a valid authorisation from the intermediated company in Country A (either via central authorisation register (3a) or authorisation attestation (3b)) before the intermediary can request a VAT ID certificate on the intermediated company's behalf.
	b. Must support the protocols specified by each Tax Administration.
EUDI Wallet provider	a. Non-specific for BU3 - Must enable OpenID4VP interactions
	b. Non-specific for BU3 - Must verify credentials for integrity, authenticity, trust status, and revocation status
	c. Non-specific for BU3 - Must integrate with trusted lists and credential validation services
PID Provider	a. Where applicable, must issue PID containing both mandatory, and optional attributes depending on Member States. Each Tax Administration defines the identity data required for scenario 1.
	b. Where applicable, non-specific for BU3 - Must support secure PID issuance, renewal, and revocation
	c. Where applicable, non-specific for BU3 - Must provide up-to-date status information for trust and revocation need.
Trusted list registrar	a. Non-specific for BU3 - Must maintain and publish trusted lists
	b. Non-specific for BU3 - Must ensure trust status information is available and accessible for validation purposes.
	c. Non-specific for BU3 - Must provide machine-readable interfaces for trusted list access and consumption.
QEAA provider	a. Non-specific for BU3 – Tax Administrations piloting with QEAA must comply with generic QEAA requirements.
	b. Tax Administration is used as authentic source
Pub-EAA provider	a. Non-specific for BU3 – Tax Administrations piloting Pub-EAA must comply with generic Pub-EAA requirements.
	b. Tax Administration is used as authentic source
EAA provider	c. NA
QES provider	a. Non-specific for BU3 - QES may be supported to request VAT ID on
	b. Non-specific for BU3 – Tax Administrations must be able to seal VAT ID certificate.

Annex 2 – Intermediary obtains an authorisation attestation

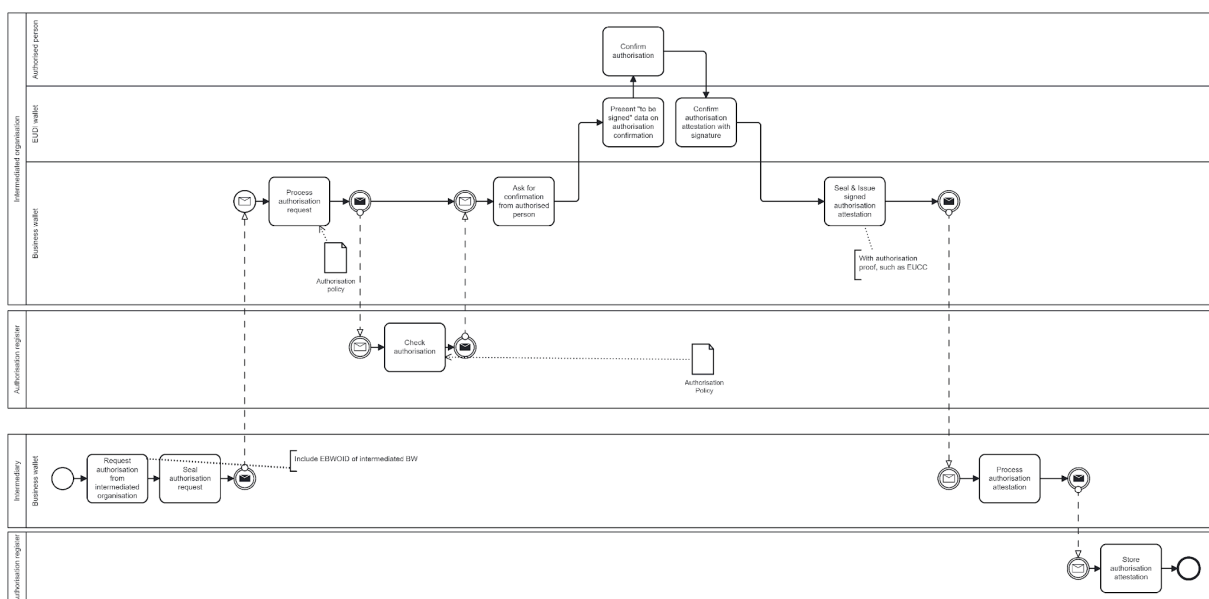
This process establishes an authorisation attestation for later use by the intermediary. The intermediary business wallet sends a sealed request to the intermediated organisation, the business wallet of the intermediated company verifies the request by accessing its authorisation register, where applicable, obtains confirmation from an authorised person via the EUDI wallet, and issues a signed and/or sealed authorisation attestation. The issued attestation is then sent back to the intermediary business wallet and stored in an authorisation register.

A prerequisite for this process is that the intermediary is registered in the authorisation register of the intermediary process. This bootstrap process is explained in scenario 1, annex 2 for natural persons and can be re-used for registering intermediaries.

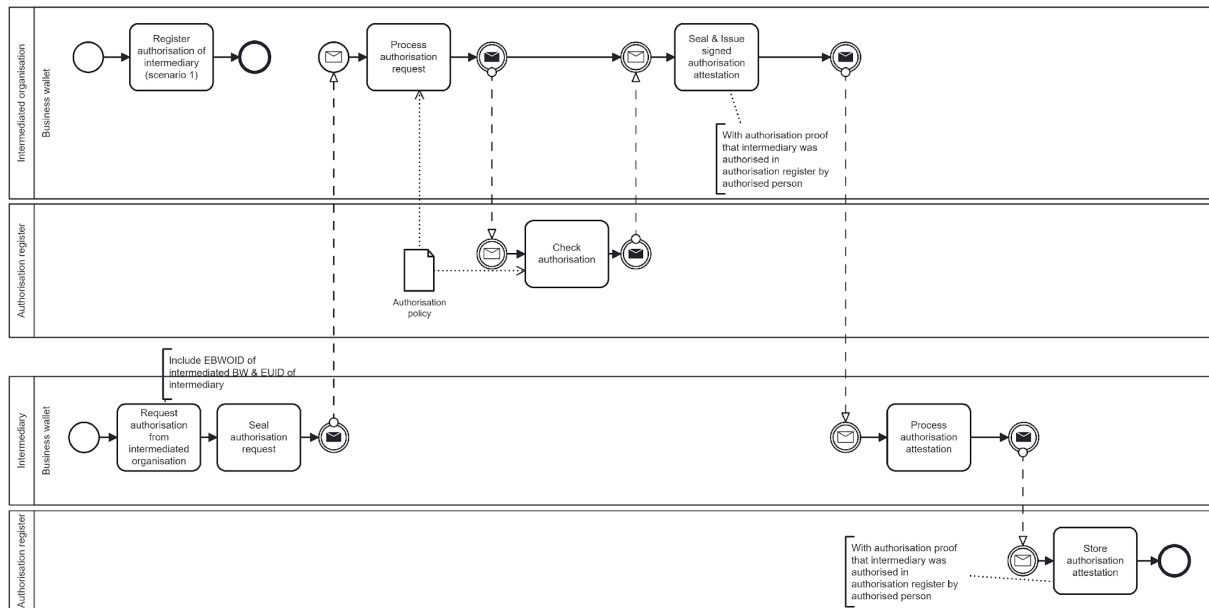
While qualified electronic signatures may not always be required, the capability of an EUDI wallet makes this a highly relevant perspective. It introduces non-repudiation, which becomes particularly valuable if the register serves an external function, for example as part of a business wallet, where it can also provide a foundation for issuing attestations based on the register. This effectively turns it into a generic function that can be reused within the business wallet (**subscenario 4b-1a**). In full system-to-system interactions, an entry may alternatively be considered authentic when it is sealed with a qualified electronic seal (**subscenario 4b-1b**).

It is therefore important to note that this register, if it becomes part of a business wallet or is operated by an external trusted party, may also contain the proof or authorisation information regarding individuals who are permitted to manage and modify the register for specific services, such as authorisation of intermediaries in their authorisation register. This way, the chain of authorisation in authorisation attestations issued to intermediaries and applied in VAT declaration or VAT ID certificate issuance processed, can be validated by the Relying Party of Issuer. This enables a layered or hierarchical authorisation model.

Subscenario 4b-1a - Issuance of authorisation attestation with Qsig



Subscenario 4b-1b - Issuance of authorisation attestation with Qseal



webuild-consortium / BU4

Type to search

Code

Issues

Pull requests2

Agents

Actions

Projects

Security and quality

BU4 / scenarios / 1A-PoA-Issuance /



borislingl

Revise entities in PoA Issuance README

b61483d · 2 days ago

History

Name	Name	Last commit date
..		
README.md	Revise entities in PoA Issu...	2 days ago

README.md

Scenario 1A — Issuance of a Power of Attorney Attestation

MVP Scenario



WE BUILD

CONSORTIUM

Specification Scenario BU4 1a – Issue a PoA

WP2 – UC BU4 1a – Issue a PoA

Date : 21/07/2026

Version : 1.1 (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)

Status : Draft (Draft, for review, reviewed, final)

Index

1 Introduction

1.1 Objectives of this document

1.2 Scenario introduction

2 Scenario specification

2.1 Introduction

2.2 Scenario pre-conditions

2.3 Scenario main flow

2.4 Scenario additional flows

2.5 Challenges and barriers

2.6 Working Assumptions

3 Detailed scenario flow

4 Roles and participants

4.1 Scenario roles and participants

4.2 Additional roles and partners

4.3 Target country combinations

4.4 Requirements

5 Attestations

5.1 Introduction

5.2 Attestations to be provided by other UCs/WGs/scenarios

5.3 Created attestations in the scenario

Annex 1

[Annex 1 – Requirements for scenario roles]

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario **"Issue a Power of Attorney (PoA)"**, as part of the use case "Company representative acting on behalf of company" [BU4] in work package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

Explain the scenario in one line, describing what will be piloted cross border.

A natural person uses a Business Wallet containing Power of Representation (PoR) and/or Power of Attorney (PoA) attestations to prove authorization to act on behalf of a legal entity and access digital services provided by cross-border public or private relying parties.

The scenario is based on the following documentation:

- Include references to ARF version

- Include references to Stock Taking document
<https://portal.webuildconsortium.eu/group/bu4-company-representative-acting-behalf-company/files?mid=5839&fid%5B0%5D=88&fid%5B1%5D=89&fid%5B2%5D=4194>
- Include references to relevant WP4 documentation <https://github.com/webuild-consortium/wp4-architecture>
- Include references to relevant 1st generation documentation
- Include references to relevant domain documentation <https://github.com/webuild-consortium/wp4-architecture/tree/main/adr>

2 Scenario specification

2.1 Introduction

// MVP-UseCase based on EUBW, authenticated User towards EUBW by EUDIW //

The issuance of a power of attorney in an EUBW enables a person to act on behalf of an organization in a controlled and legally valid way. This is important because many business and administrative processes require an authorized individual to make declarations, submit requests, or receive information for the organization. By formalizing this delegation, the organization ensures that actions are traceable, properly authorized, and accepted within the relevant digital process.

At a high level, the process begins with the organization defining who should be granted authority and for which specific purpose. The power of attorney is then prepared, approved, and issued so that the representative can perform the intended actions within the EUBW environment. This creates a clear and trusted link between the organization and the acting individual, reducing ambiguity and supporting secure digital operations.

The issuance process typically starts with the organization authenticating itself toward the EUBW using an EUDI-based trust mechanism. Once the organization is securely identified and authorized, the relevant credentials can be issued and bound to the organization's wallet or digital identity context. This creates a trusted foundation for further actions, such as representing the organization and executing controlled business processes.

Later use the issued credentials to get access to service scenario: Use of PoA and/or PoR attestations for access to commerce platforms, public platforms, get payment or balance sheets at banks and other situations that require representation of companies.

This scenario is part of the MVP scope of BU4 and focuses on the use of representation credentials for accessing cross-border services.

Wallets used in the scenario:

- Business Wallet (EUBW): used to store, verify, present and issue company related mandates (preferred scenario)
- EUDIW for EAA presentation in combination with PID or QEAA / PubEEA (depending on jurisdiction in EU member state)

2.2 Scenario pre-conditions

For the Use Case to succeed there are several conditions that have to be met on top of the ones that have to be developed in the Use Case itself:

- Availability of a EUIDW that incorporates the PID of the person acting on behalf of the company or containing a person with a professional state (e.g. tax advisor).
- Availability of a EBW that incorporates the EBWOID of the company that is going to perform the cross-border operations.
- Availability of Authentic Sources (AS) holding the core data that is going to be included in the attestation of attributes.
- Capability to use later a QERDS communication channel (MVP+)

- Capability of the (Q)TSPs to issue the PoA and PoR attestations in the EUBW, including a clean definition of the issuance process (required inputs, verification steps, and supporting documents such as PID, EU Company Certificate, and company statutes).
- Capability of the relying party to be able to verify issuer trust, signature validity, status, and scope.

2.3 Scenario main flow

Main flow:

1. User opens wallet(s)
2. User opens EUBW wallet interface
3. Verification request from EUBW instance

Note over User, EUBW : here we use an EUDIW, could also be another method like using your plastic id card with an app

4. User opens his/her EUDIW and presents PID
5. User present PID towards EUBW -> we expect that to be successful (OK)
6. EUDIW towards EUBW: present PID information towards EUBW – we expect a successful verification result
7. User request for PoA Issuance, e.g. if more than one the PoAIssuer displays a list of available PoA types and attestable mandateship relations
8. User selects PoA
9. AuthenticSource and PoAIssuer connection established
10. PoAIssuer requests information from authentic source
11. AuthenticSource provides information to PoAIssuer
12. PoAIssuer, User: issue PoA and PoAIssuer presents credential offer via deeplink
13. User accepts credential via deeplink and

EUBW establishes connection via deeplink

14. PoA issuance request (including wallet instance ID, LPID reference, requested attributes), PoAIssuer towards TrustInfrastructure**:** Verify wallet instance and issuer authorization

15. TrustInfrastructure towards PoAIssuer: Confirmation of wallet and issuer trust status (if needed)

Note over PoAIssuer: tax advisor mandates are stored in a separate database

PoAIssuer towards User: Request strong user authentication and mandate details e.g. stored in separate database

16. User provides authentication to PoAIssuer (eID, QES, or national eID) and mandate data

Note over User, PoAIssuer: authentication provided

PoAIssuer towards PoAIssuer: Validate identity, mandate scope, validity period, and legal basis

17. PoAIssuer optionally checks company / legal person register and mandate registers

18. TrustInfrastructure returns towards PoAIssuer: Return company, professional state, mandate information

19. PoAIssuer creates digital Power of Attorney as electronic attestation of attributes (EAA / PID / LPID / mandate relation)

20. PoAIssuer towards TrustInfrastructure: sign/seal EAA

TrustInfrastructure towards PoAIssuer: transmit signed/sealed EAA (QEAA)

21. PoAIssuer issues signed PoA credential to wallet (via EUBW issuance API)

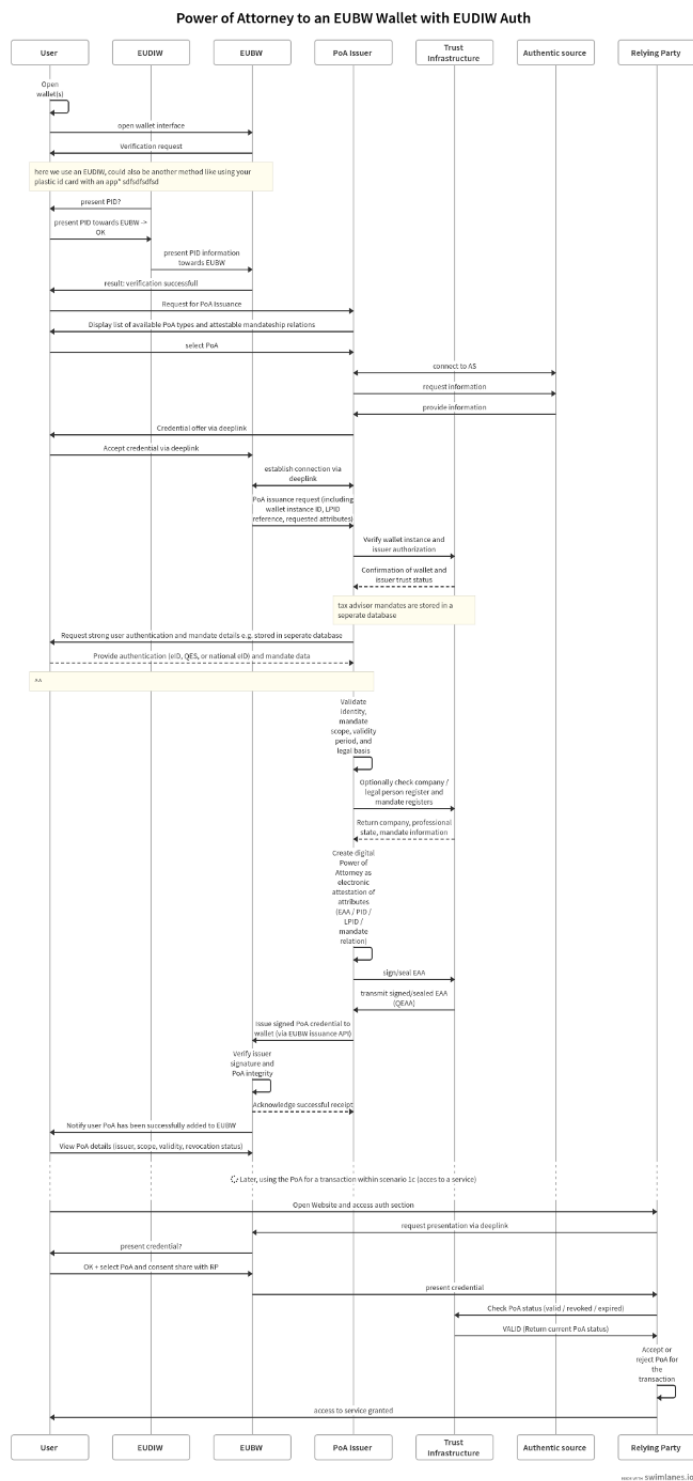
22. EUBW verify issuer signature and PoA integrity

23. EUBW acknowledge successful receipt

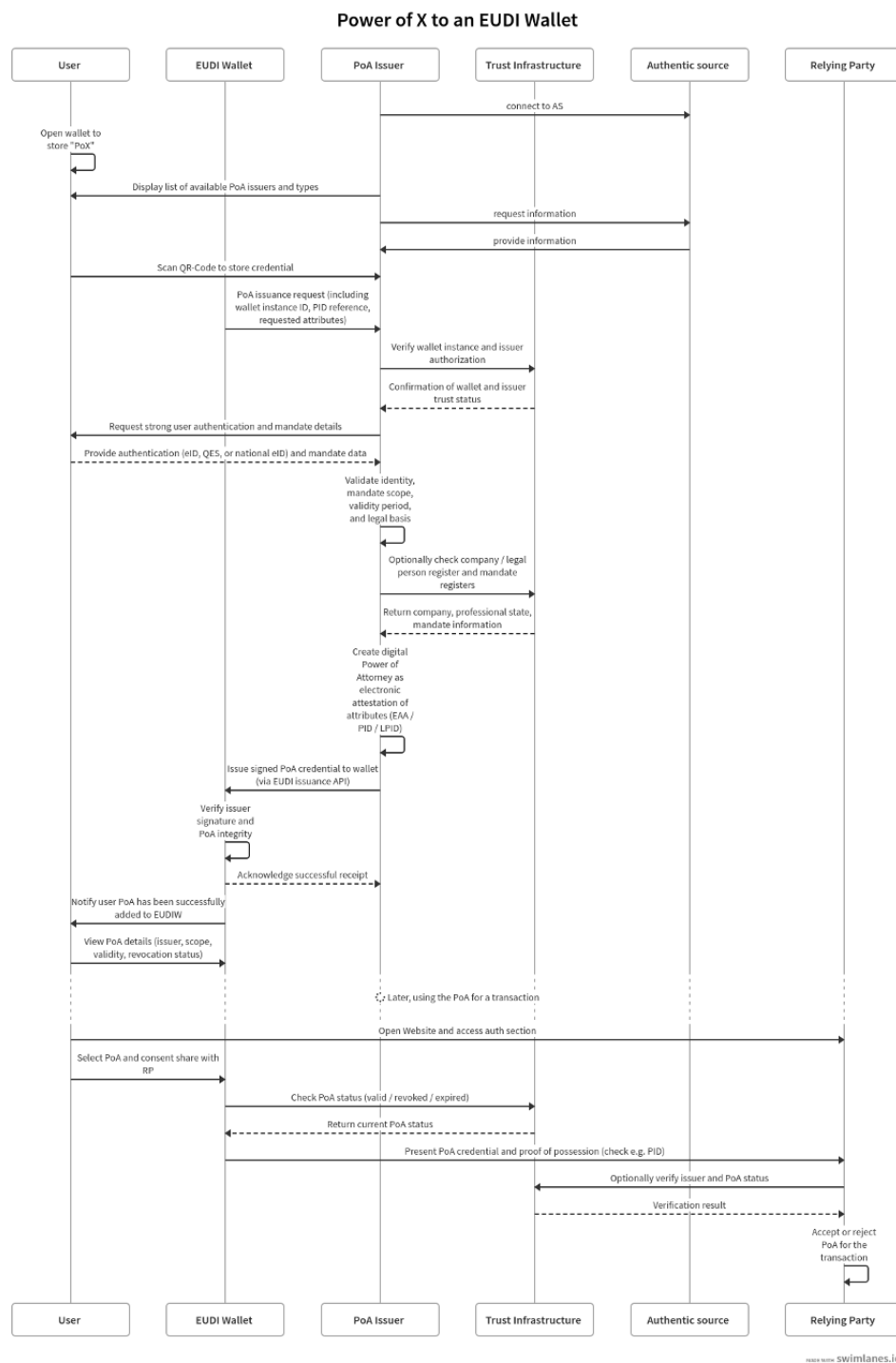
24. EUBW notifies user PoA has been successfully added to EUBW

25. User could view PoA details (issuer, scope, validity, revocation status)

Please refer to swimlane //REFERENCE-URL <https://github.com/webuild-consortium/BU4/blob/main/scenarios/diagrams/poa-issuance-sequencediagram.mmd>



Please refer to swimlane **//REFERENCE-RUL** <https://github.com/webuild-consortium/BU4/blob/main/scenarios/diagrams/pox-eudiw-issuance.mmd>



2.4 Scenario additional flows

A scenario may include certain variations of the main flow execution that the use case wants to pilot cross border. Like same device vs cross device execution.

A scenario may also want to address certain exceptions to the main basic flow. Like a user not having the proper mandate, diplomas, IBAN etc.

These can be mentioned in the table below, but only those that the use case really aims to pilot (so not every thinkable exception needs to be mentioned here, if the use case will not pilot that anyway. These may include several technical exceptions that need to be tested, but not explicitly piloted: these do not need to be included in the table below).

Flow	Short description
Variations	
•	Scenario with required QEAA (depending on service requirements) Note: not sure it applies to this scenario. To be discussed
•	Access to the service via intermediary RP (e.g., platform acting as RP intermediary)
Exceptions	
•	User does have a valid PID in order to use together with EAA (if needed)
•	User does not have valid PoA / PoR for the legal entity
•	Credentials are expired or revoked
•	Wallet cannot access QES provider when signature is required
•	LPID missing or not trusted by RP
•	Cross-border trust failure (issuer not recognized in another country)

If helpful, it can be made explicit what will NOT be piloted cross border. This should be in line with section 1.4 of the Stock Taking document.

(Copy/Paste from Stock Taking 1.4 – not sure we should consider it)

This Use Case will not consider any of the following situations or areas:

- Mandates that do not require formal appointment and registration in an authentic source. (e.g. mandates based on a contract)

- Mandates that are not based on European Regulation or a Member State national regulation (e.g. mandates based on the role within the company such as purchasing capabilities for the CFO).
- The foundation for this LSP is the current state of the EUDI Architecture and Reference Framework (ARF) and the corresponding EU Implementing Acts. Especially in a business context, a future EU Business Wallet could provide significant added value by enabling end-to-end process automation and greatly facilitating the use of PoA and PoR. However, since these specifications are still in the planning phase, their complete application within the pilot is not expected at this stage.
- The foundation for this LSP is the current state of the EUDI Architecture and Reference Framework (ARF) and the corresponding EU Implementing Acts. Especially in a business context, a future EU Business Wallet could provide significant added value by enabling end-to-end process automation and greatly facilitating the use of PoA and PoR. However, since these specifications are still in the planning phase, their complete application within the pilot is not expected at this stage.

2.5 Challenges and barriers

Describe the main challenges and barriers that are expected concerning the development of the solution needed for piloting the scenario. You can use the Stock Taking document sections 1.7, 4.2, 5, and 6 as a basis.

- **Interoperability of Wallets** – Multiple wallets (Natural Person Wallet, Business Wallet) need to interoperate across borders and across different RP platforms. Early testing is necessary to identify integration issues.
- **Lack of harmonization of attestations** – Differences in PoA, PoR, EU Company Certificate formats and authentic sources may create inconsistencies across countries.
- **Availability of authentic sources / registers** – Some business registers or trusted sources may not be accessible or updated in real time, impacting credential verification.

- **Dependency on emerging standards** – Certain standards (e.g., ETSI TS 119 478 for authentic sources) are still in draft form, and specifications may change, affecting implementation. [TBC]
- **Qualified Electronic Signature integration** – Wallets must reliably interface with QES providers; network, certification, or API issues may impact cross-border signature generation.
- **Evolving EU framework** – Regulations and implementing acts (eIDAS 2, EUDI Wallet regulations, Directive (EU) 2025/25) are recently published or still evolving, which may require adjustments to the solution to remain compliant.
- **Mandates that do not require formal appointment** and registration in an authentic source (e.g. mandates based on a contract)

2.6 Working Assumptions

In case of significant uncertainties, working assumptions can be installed to establish ‘a stable foundation’ for the development of the scenario. The uncertainty may relate to (project) internal or external aspects, like the (future) availability of guidance on certain aspects in the ARF. In this case, the scenario may choose a direction for development, that is expected to be chosen in a future ARF as well.

3 Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	V
Open wallet / wallet interface	User, EUDIW	The user opens the wallet, typically from the web flow or via an app/deep-link context.	Wallet is installed and available; user has access to the device.	If 1 nc alt pa

Open wallet interface / verification request	EUDIW, EUBW	The website or browser frontend starts the verification process and sends a verification request to the wallet / EUDI wallet context.	Browser session; connection between the website and the wallet environment.	Th als alt wi ca ap
Present PID / present PID info	User, EUDIW, EUBW	The wallet presents the PID to EUBW, and the PID information is then transferred for verification.	PID available in the wallet; valid wallet instance.	If t mi inv ve
Verification successful	EUBW	EUBW confirms that the verification was successful.	Successful validation of the PID data.	If v fai sto to sto
Request for PoA issuance	EUBW, PoA Issuer	EUBW requests available PoA types and mandate relationships from the PoA Issuer.	Trust relationship between EUBW and PoA Issuer; access to PoA metadata.	Th ma mi tyl ma va
Display list of available PoA types and attested mandate relationships	EUBW, User	The available PoA types and attested mandate relationships are shown to the user.	Response from the PoA Issuer.	Th en ma ex
Select PoA	User, EUBW	The user selects a specific PoA type.	Display of selectable PoAs.	Th ca an
Connect to		The PoA Issuer connects to an	Access to the	De

AS / request information / provide information	PoA Issuer, Authentic source	authentication/authentic source and requests information; the source provides the information.	authentic source; technical connection.	the information conditions
Credential offer via deeplink	PoA Issuer, EUBW	The PoA Issuer sends a credential offer via deeplink to the wallet / EUDI wallet flow.	Deeplink capability; correct wallet context.	If a wallet is available
Accept credential via deeplink	User, EUDIW	The user accepts the credential offer via the deeplink.	User interaction; active wallet context.	The wallet is ready to use
Establish connection via deeplink	EUDIW, PoA Issuer	The wallet establishes a connection to the PoA Issuer via the deeplink.	Accepted credential offer; working deeplink session.	The wallet is connected to the PoA Issuer
PoA issuance request	EUDIW, PoA Issuer	The wallet sends the PoA issuance request, including wallet instance ID, URN reference, and requested attributes.	Previous connection; required technical identifiers.	Reactivation of the wallet
Verify wallet instance and issuer authorization	PoA Issuer, Trust Infrastructure	The PoA Issuer verifies the wallet instance and its own authorization.	Trust infrastructure; validation mechanisms.	If a wallet is available for issuance
Confirmation of wallet and issuer trust status	Trust Infrastructure, PoA Issuer	The trust chain and the status of wallet and issuer are confirmed.	Trust service / trust infrastructure.	Available for issuance
Request		The wallet requests	Available	

strong user authentication and mandate details	EUDIW, PoA Issuer, User	strong authentication and mandate data, for example stored in a separate database.	authentication method; mandate data present.	De th ad ma
Provide authentication and mandate data	User, EUDIW	The user provides identity/authentication data and mandate data.	Successful strong authentication; access to mandate data.	Th m ex as na
Validate identity, mandate scope, validity period, legal basis	PoA Issuer	The PoA Issuer validates identity, mandate scope, validity period, and legal basis.	Submitted authentication and mandate data.	Ve fai ba or ha
Optionally check company / legal person register and mandate registers	PoA Issuer, Trust Infrastructure	Additional verification against company or mandate registers.	Access to registers; trust infrastructure.	Op de gc tru
Return company, professional state, mandate information	Trust Infrastructure, PoA Issuer	Registry or verification information is returned.	Successful register lookup.	Th be a i un
Create digital Power of Attorney / attest mandate	PoA Issuer	The PoA Issuer creates the digital power of attorney or attests the mandate relationship based on the attributes.	Successful validation; confirmed mandate data.	Th de de th

relation				
Sign / seal EAA	PoA Issuer	The EAA is signed or sealed.	Suitable signing/sealing mechanism.	If I se av pr be
Transmit signed/sealed EAA (QEAA?)	PoA Issuer, EUDIW	The signed/sealed EAA is transmitted to the wallet.	Successful signing/sealing; transport channel.	Th su "G pc inc qu
Issue signed PoA credential to wallet via EUBW issuance API	EUDIW, EUBW	The wallet receives the signed PoA credential via the EUBW issuance API.	Working issuance API; valid EAA.	AF sc mi ab iss
Verify issuer signature and PoA integrity	EUDIW	The wallet verifies the signature and integrity of the PoA.	Received credential; matching trust parameters.	In sig to
Acknowledge successful receipt	EUDIW, PoA Issuer	Successful receipt is acknowledged.	Successful validation and storage.	If nc ac is
Notify user PoA has been successfully added to EUBW	EUDIW, User	The user is informed that the PoA was successfully added to the wallet / EUBW.	Successful issuance.	In an m sh
View PoA details	User, EUDIW	The user can view details such as issuer, scope, validity, and	Stored PoA credential.	Th de m

		revocation status.		
Open website and access auth section	User, Relying Party	Later, the user uses the PoA for a transaction and opens the website or authentication section.	Existing PoA; relying party website.	Th ha tin im
Request presentation via deeplink	Relying Party, EUDIW	The relying party requests a presentation of the PoA via deeplink.	Deeplink support; active wallet session.	If c av alt pr flc
Present credential	EUDIW	The wallet presents the credential to the relying party.	Previous presentation request.	Pr ma or
Check PoA status (valid / revoked / expired)	Trust Infrastructure, Relying Party	The status of the PoA is checked.	Access to status / revocation information.	If i ex tra re,
VALID (return current PoA status)	Trust Infrastructure	The current status is returned.	Successful status lookup.	Ca re ex
Accept or reject PoA for the transaction	Relying Party	The relying party accepts or rejects the PoA for this transaction.	Status check result and policy rules.	Re oc sc ex lac
Access to service granted	Relying Party, User	If the check succeeds, access to the service is granted.	Valid PoA; accepted presentation.	If i va de

4 Roles and participants

4.1 Scenario roles and participants

Describe the roles relevant for this scenario, and list which of the partners will play this role in piloting the scenario. Note that the roles primarily active in the use case are mentioned. Section 1.5 of the Stock Taking document can be used as a basis.

Primary role	UC partner Name	Country
1. User of EUBW Wallet	tax advisor acting on behalf of organisation handing in declaration(DATEV)	DE
2. Authentic sources	DATEV / Telekom / Notariado	DE / ES
3. Relying party	Tax Authority (accepting tax declarartion in from tax advisor) / Notariado	NL / DE / ES
4. Intermediary		

4.2 Additional roles and partners

Describe which partners that primarily work in WP4 participate in piloting this scenario. Section 3 from the Stock Taking document can be used as a basis.

Primary role	UC partner Name	Country	Wallet
1. EUBW Wallet provider	PROCIVIS		
	CREDENCO	DE	
	iGrant	NL	

	Siros		
2. PID Provider	BDR Bolagsverket	DE SE	
3. Trusted list registrar	IDunion	DE	
4. QEAA provider	Registradores T-Systems / DTAG Cleverbase Docaposte Intesi	ES DE DE FR FR IT	
5. Pub-EAA provider			
6. EAA provider	Registradores T-Systems / DTAG DATEV Cleverbase Docaposte Intesi	ES DE DE FR FR IT	
7. QES provider			

Scenario ID	Relying Party		Issuer			N
	Ctry	RP Name	Ctry	Issuer Name	Attestation(s)	
MVP						

1a	FR	Docaposte			PoA, PoR	
	IT	InfoCamere SCpA			PoA, PoR	InfoC SCpA
	FR	Infogreffe			PoA, PoR	
	ES				PoA, PoR	IZER
	BE	OpenPeppol AISBL			PoA, PoR	Orar
	SE	Skatteverket	SE	Bolagsverket	PoR	
	DE					IDun SCE
	IT					Page
	GR	GRNET	GR	GRNET	PoA, PoR	GRN

4.3 Target country combinations

Because WE BUILD is a cross-border pilot but not all countries may want to pilot with all other countries, state which countries intend to pilot the scenario with each other.

	Issuing country						
		ES	NL	DE	ES	FR	...
Relying Party country	AT						
	BE						
	DE	X	X	X	X		
	NL	X			X		
	FR						

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Declare which attestations will be used in the scenario, but will NOT be designed, implemented and issued to wallet within the scenario

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Personal Identification	BDR	DE	
LPID & EBWOID	LPID or EBWOID	BANZ	DE	

5.3 Created attestations in the scenario

Describe the attestations what will be created by issuers, within the scenario (so these are not the 'foreign' attestations).

Note that for each of the attestations, a rulebook must be made during the specification phase.

- Each rulebook will be made in collaboration with the SEMANTICS workgroup from WP4. An example rulebook is provided, of which the Use Case shall create sections 1, 2 and 3 while WP4 SEMANTICS creates the sections 4 and onwards.
- We aim for fit-for-pilot attestations. Each rulebook describes the set of attestations the as agreed upon by the scenario partners from the perspective of requesting and providing, that are relevant for piloting the scenario. The rulebook shall not include attributes that either none of the relying parties need, or none of the issuers can provide for piloting the scenario, unless existing domain-standards that are adopted, dictate otherwise.

State which countries will create these attestations and ensure that this is aligned with the targeted country combinations in section 4.4 of this document.

Attestation name	Short description	For Countries	Applicable domain standards
Power of Attorney	power of attorney is a legal document that lets one person act on behalf of another	DE	

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUBW Wallet	a. Have a EUBW with an OID in it
	b.
	c.

2. Authentic sources	a. Available to issue credentials – here e.g. a tax advisor id
	b. provides data for credentials according to rulebook id
	c.
3. Relying party	a. Having a EUBW and Portal set up
	b. Ready to accept credentials
	c.
4. Intermediary	a. Possibility to issue/verify and forward information
	b. Interaction has to be defined (probably not needed for issuing a PoA)
	c.
5. EUDI Wallet provider	a. Users should have a valid EUDIW instance, in order to auth against EUBW
	b.
	c.
6. PID Provider	a. Ready to issue and store PID to EUDIW
	b. EUDIW ready to present towards a EUBW
	c.
	a. Up and running Status & TruvsList infrastructure

7. Trusted list registrar	
	b.
	c.
8. QEAA provider	a. Ready to issue a QEAA – OR --
	b. Ready to seal pubEAA
	c.
9. Pub-EAA provider	a. Ready to issue pubEAA
	b. Have a QTSP Role in order to seal pubEAA
	c.
10. EAA provider	a. Ready to issue a EAA towards EUDIW
	b. Ready to issue EAA towards EUBW
	c.
11. QES provider	a. Availability (if needed) to sign document (not needed at the moment for issuing a PoA)
	b.
	c.

webuild-consortium / BU4

Type to search

Code

Issues

Pull requests2

Agents

Actions

Projects

Security and quality

BU4 / scenarios / 1B-PoR-Issuance

 **borislingl**

Update date and version in README.md

dd6a5a1 · 2 days ago

 History

Name	Name	Last commit date
..		
README.md	Update date and version i...	2 days ago

README.md

Scenario 1B — Issuance of a Power of Representation Attestation

MVP Scenario



WE BUILD

CONSORTIUM

Specification Scenario BU4 1b – Issue a PoR

WP2 – UC BU4 1b – Issue a PoR

Date : 21/07/2026

Version : 1.1 (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)

Status : DRAFT (Draft, for review, reviewed, final)

Index

1 Introduction

1.1 Objectives of this document

1.2 Scenario introduction

2 Scenario specification

2.1 Introduction

2.2 Scenario pre-conditions

2.3 Scenario main flow

2.4 Scenario additional flows

2.5 Challenges and barriers

2.6 Working Assumptions

3 Detailed scenario flow

4 Roles and participants

4.1 Scenario roles and participants

4.2 Additional roles and partners

4.3 Target country combinations

4.4 Requirements

5 Attestations

5.1 Introduction

5.2 Attestations to be provided by other UCs/WGs/scenarios

5.3 Created attestations in the scenario

Annex 1

[Annex 1 – Requirements for scenario roles]

1 Introduction

1.1 Objectives of this document

This document describes the details of **scenario 1b – Issuance of Powers of Representation (PoR) attestations to a EU Business Wallet**, as part of use case **BU4** in **work package 2** in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

Explain the scenario in one line, describing what will be piloted cross border.

This scenario pilots the issuance of a Powers of Representation (PoR) attestation to a EU Business Wallet (EUBW) or EUDI Wallet (EUDIW), enabling the person, either natural or legal, to prove they are authorized to represent a company in digital interactions.

The PoR attestation is issued based on information held in authentic sources, such as Business Registries, and is issued by a Qualified Trust Service Provider (QTSP) acting on behalf of an authentic source, or by a public sector body responsible for an authentic source.

The attestation links:

- The Natural or Legal Person that acts on behalf of the Company (Proxy)
- The Economic Operator (identified via EBWID, previously known as LPID), known as the Legal Entity Represented.
- The representation powers granted and all the contextual information such as limitations.

While the scope of this scenario is limited to the issuance and use of the PoR attestation for representation purposes as described above, it is intended to serve as a foundational building block for future use cases, where this attestation can be reused or extended in broader digital interactions involving legal person representation.

The attestation can subsequently be presented to relying parties to perform actions on behalf of the company.

The scenario is based on the following documentation:

- Include references to ARF version
- Include references to Stock Taking document
<https://portal.webuildconsortium.eu/group/bu4-company-representative-acting-behalf-company/files?mid=5839&fid%5B0%5D=88&fid%5B1%5D=89&fid%5B2%5D=4194>
- Include references to relevant WP4 documentation
- Include references to relevant 1st generation documentation
- Include references to relevant domain documentation <https://github.com/webuild-consortium/wp4-architecture/tree/main/adr>

2 Scenario specification

2.1 Introduction

Provide a high level introduction of the scenario. Possibly copy-paste this from the Stock Taking document.

Declare under which UC this scenario resides and if the scenario is part of the MVP or MVP+.

Declare if the scenario will use a Natural Person Wallet, a legal Person Wallet or both.

Scenario 1b focuses on the issuance of Powers of Representation (PoR) attestations to a Natural Person and/or a Legal Person, defined in this context as Proxy.

The attestation proves that a Proxy is entitled to act on behalf of a legal entity in certain business contexts.

This scenario resides under **WP2 – Business Use Case 4 (BU4)** and is part of the **MVP scope**.

The scenario uses:

- Legal Person Wallet (European Business Wallet)
- Legal Person identifiers (EBWOID)
- Electronic Attestations of Attributes

2.2 Scenario pre-conditions

Detail the relevant pre-conditions from the Stock Taking document, section 1.6.

The following conditions must be fulfilled before the scenario can be executed:

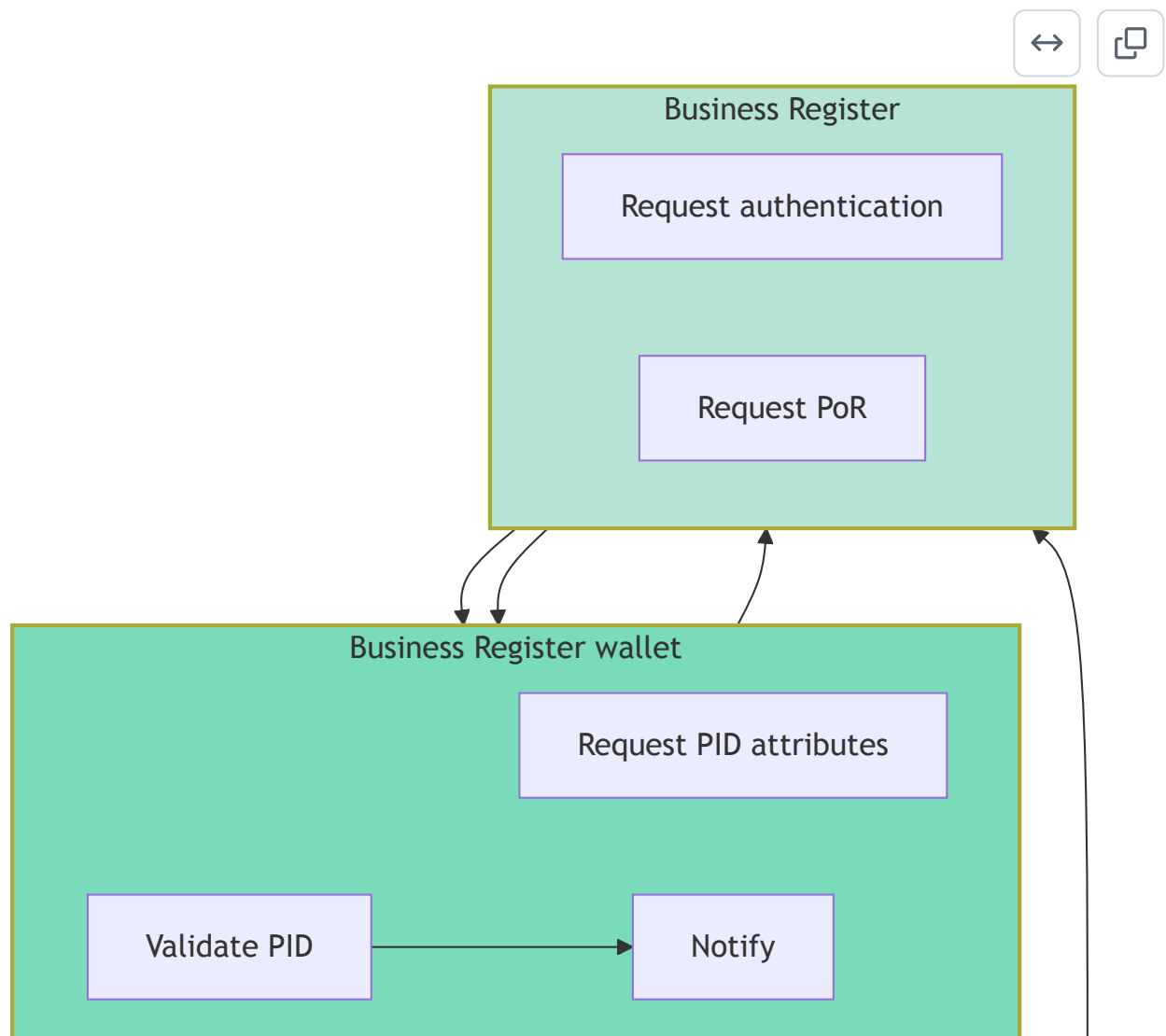
1. The company is registered in a Business Registry or another authentic source capable of confirming representation powers.
2. The company involved has a Legal Person Identifier (EBWOID, previously known as LPID) available in their Company's European Business Wallet (EUBW).
3. The Business Registry or authentic source has the necessary information that is needed for the issuance of the Power of Representation.
4. The Issuer (QTSP) has the technical capability to issue and verify Electronic Attestation of Attributes and can also query the Authentic Source for the information needed.

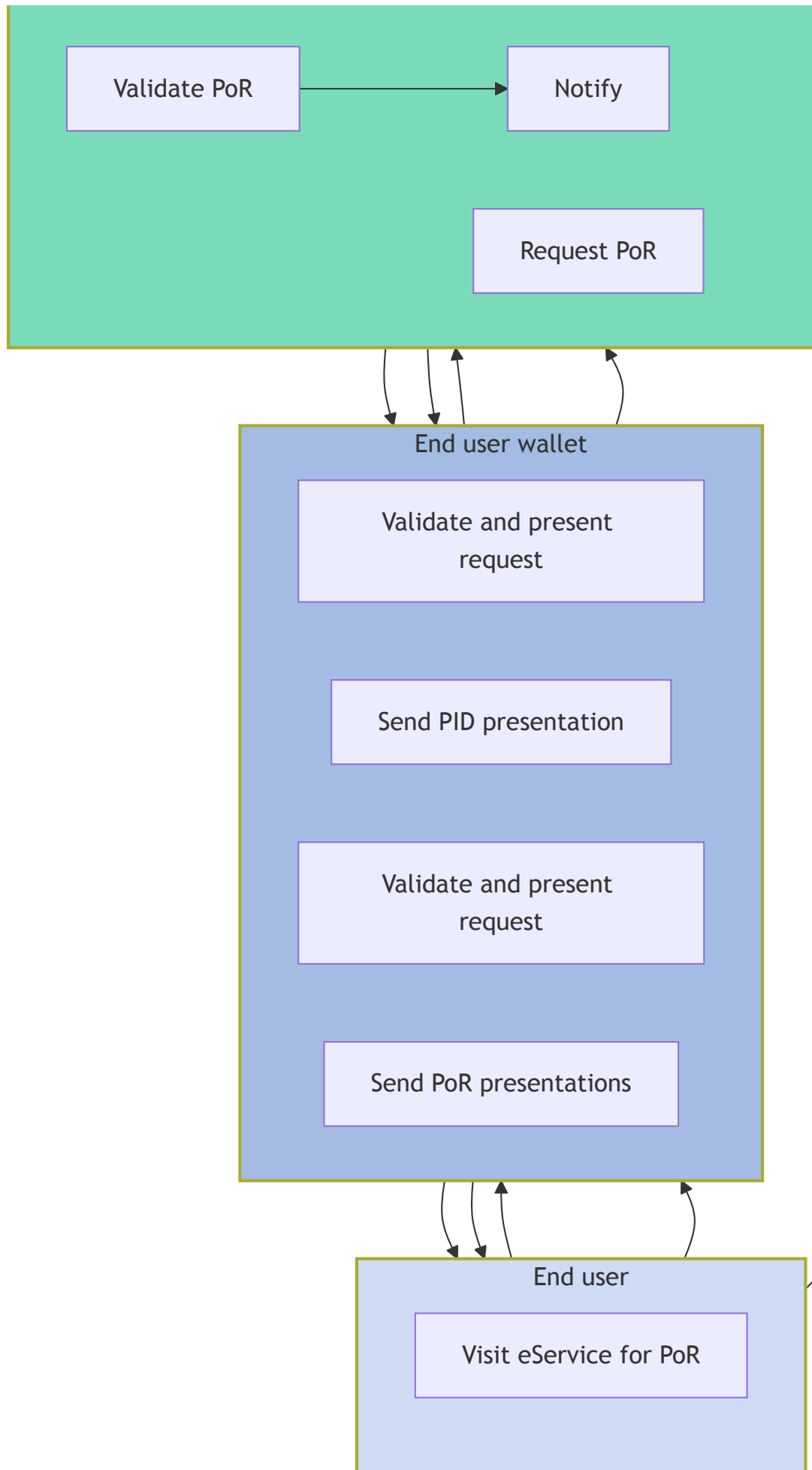
5. The relying parties participating in the pilot support verification of Electronic Attestations of Attributes and have the integrations done with their own European Business Wallet.
6. The user is already registered in the Company's European Business Wallet, and is logged in.

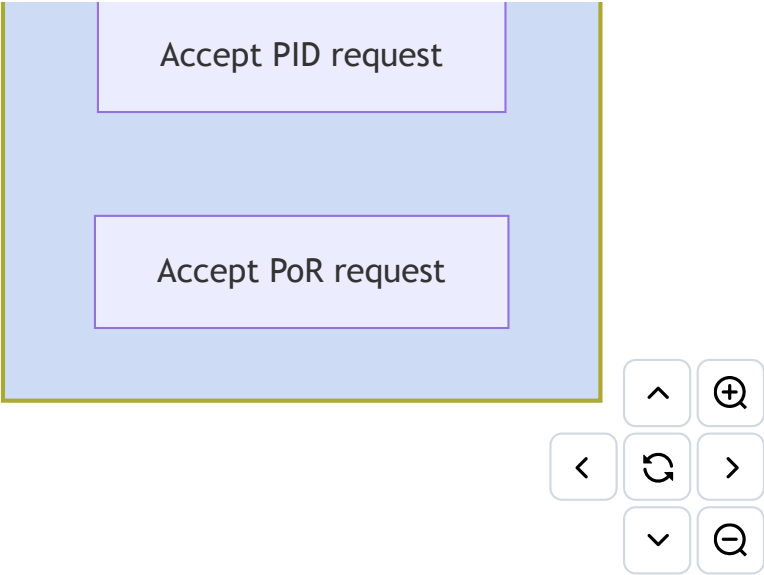
2.3 Scenario main flow

Provide a swimming lane diagram of the one main process flow that will be piloted cross border, to mark the beginning, ending and most important steps. Constrain to the following swimming lanes : User (incl wallet), Relying Party (may be split into intermediary and relying party), (Q)EAA or Pub-EAA provider, QES provider, (L)PID provider.

BPMN – Diagram:







Main flow step -same- device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
1. Visit eService for PoR	End user	Natural person designated as managing director of branch visits the eService of the Business Register in the member state the foreign company wants to register a branch.		
2. Request	Business	The Business Register requires end users to authenticate before accessing the application for branch registration. A QR		

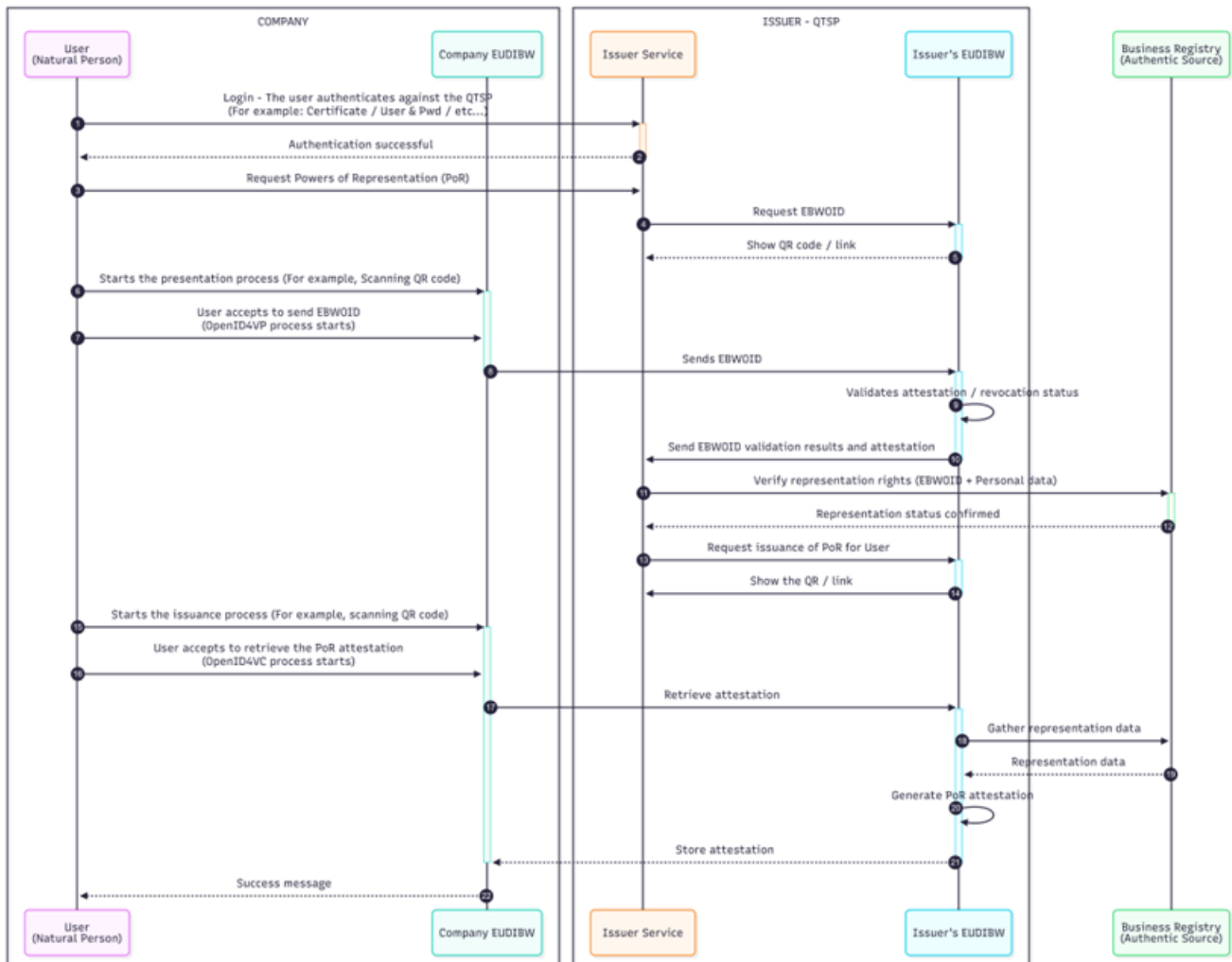
authentication	Register	code for authentication through EUDIW is presented at eService. End user scans QR code with EUDIW.		
3. Request PID attributes	Business register wallet	EBW of Business Register sends request for PID attributes to end user wallet.		
4. Validate and present request	End user wallet	EUDIW of end user validates the request from EBW and presents it to end user in EUDIW.	EBWOID - WP4 PID/LPID, BWIA/BWUA - WP Wallet providers.	
5. Accept PID request	End user	End user accepts request.		
6. Send PID presentation	End user wallet	EUDIW creates presentation and sends to EBW.	PID - WP4 PID/EBWOID.	
7. Validate PID	Business Register wallet	EBW validates PID presentation.	PID - WP4 PID/EBWOID, BWIA/BWUA - WP Wallet providers.	
8. Notify	Business Register wallet	EBW sends notification to Business Register about validated PID.		

9. Request POR	Business Register	Business Register opens eService for branch application to end user and requests POR by displaying QR codes for (each) attestation. End user scans code(s) with EUDIW.		
10. Request POR	Business Register wallet	EBW of Business Register sends request for PoR to end user wallet.		
11. Validate and present request	End user wallet	EUDIW of end user validates the request from EBW and presents it to end user in EUDIW.	EBWOID - WP4 PID/LPID, BWIA/BWUA - WP Wallet providers.	
12. Accept PoR request	End user	End user accepts request(s).		
13. Send PoR presentations	End user wallet	EUDIW creates presentation(s) and sends to EBW.		
14. Validate PoR	Business Register wallet	EBW validates PoR.	PID - WP4 PID/EBWOID, BWIA/BWUA - WP Wallet providers.	
15. Notify	Business Register	EBW sends notification to Business Register about validated		

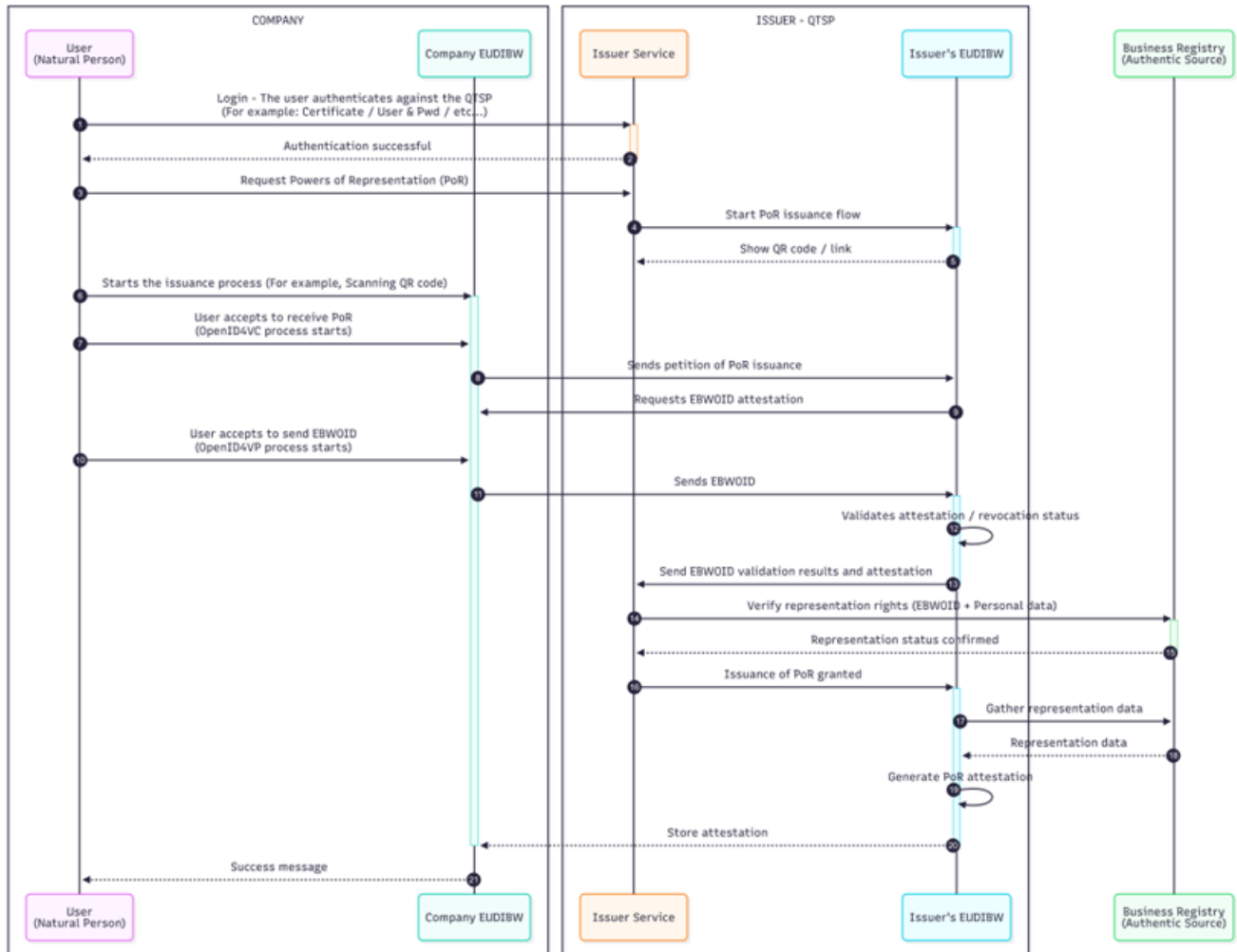
wallet	presentation(s).
--------	------------------

Flow – Diagram:

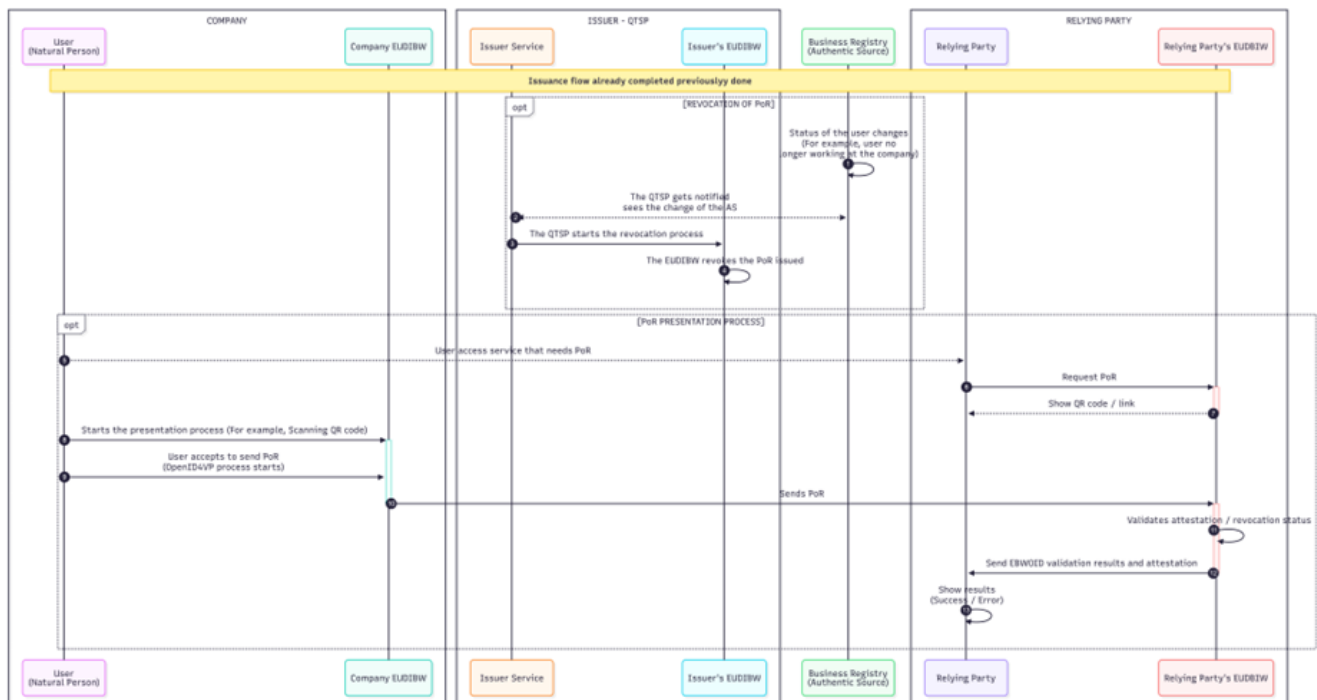
Main issuance flow:



Alternative Issuance flow:



Presentation and revocation flows



Swimlane and flow process description:

Main flow

1. The user authenticates with the Issuer Service / QTSP.
2. Once authenticated, the user requests the issuance of a Power of Representation (PoR).
3. The Issuer Service requests the Issuer's EU Business Wallet to initiate the process to obtain the EBWID.
4. The Issuer's EU Business Wallet returns a QR code or link to start the flow from the company wallet.
5. The user initiates the presentation process from the Company's EU Business Wallet by scanning the QR code or clicking the link.
6. The user consents to sending the EBWID and the OpenID4VP flow is initiated.
7. The Company's EU Business Wallet sends the EBWID to the Issuer's EU Business Wallet.
8. The Issuer's EU Business Wallet validates the presented attestation, including its status and possible revocation.
9. The Issuer's EU Business Wallet sends the validation result and the associated attestation to the Issuer Service.
10. The Issuer Service queries the Business Registry / Authentic Source to verify the user's powers of representation, using the EBWID and available personal data.
11. The Authentic Source confirms the representation status to the Issuer Service.
12. After successful verification, the Issuer Service requests the Issuer's EU Business Wallet to issue the PoR for the user.
13. The Issuer's EU Business Wallet returns a new QR code or link to initiate the issuance flow.
14. The user initiates the issuance process from the Company's EU Business Wallet.
15. The user agrees to receive the "PoR" credential, initiating the OpenID4VC flow.

16. The Company's EU Business Wallet requests the attestation from the Issuer's EU Business Wallet.
17. The Issuer's EU Business Wallet collects the necessary representation data from the Authentic Source.
18. The Issuer's EU Business Wallet generates the "PoR" attestation.
19. The Issuer's EU Business Wallet delivers the attestation to the Company's EU Business Wallet, where it is stored.
20. The wallet displays a success message to the user.

Alternative issuance method

1. The user authenticates with the Issuer Service / QTSP.
2. The user requests the PoR.
3. The Issuer Service directly initiates the issuance flow with the Issuer's EU Business Wallet.
4. The Issuer's EU Business Wallet returns a QR code or link to start the flow.
5. The user initiates the issuance process from the Company's EU Business Wallet.
6. The user agrees to receive the PoR and OpenID4VC begins.
7. The Company's EU Business Wallet requests the issuance of the PoR from the Issuer's EU Business Wallet.
8. The Issuer's EU Business Wallet first requests the EBWOID.
9. The user consents to sending the EBWOID, initiating OpenID4VP.
10. The Company's EU Business Wallet sends the EBWOID to the Issuer's EU Business Wallet.
11. The Issuer's EU Business Wallet validates the attestation and its revocation status.
12. The Issuer's EU Business Wallet sends the validation result to the Issuer Service.
13. The Issuer Service verifies the powers of representation in the Authentic Source.

14. The Authentic Source confirms the representation status.
15. The Issuer Service grants the issuance of the "PoR".
16. The Issuer's EU Business Wallet collects the representation data, generates the attestation, and delivers it to the Company's EU Business Wallet.
17. The wallet stores the credential and displays a success message.

Revocation flow

1. The user's status changes in the Authentic Source.
2. The QTSP is notified of or detects this change.
3. The QTSP initiates the revocation process with the Issuer's EU Business Wallet.
4. The Issuer's EU Business Wallet revokes the issued "PoR".

Presentation flow

1. The user accesses a service from the Relying Party that requires proof of the "PoR".
2. The Relying Party requests the "PoR" from its EU Business Wallet.
3. The Relying Party's EU Business Wallet displays a QR code or link.
4. The user initiates the presentation process from the Company's EU Business Wallet.
5. The user agrees to send the "PoR" and OpenID4VP begins.
6. The Company's EU Business Wallet sends the "PoR" to the Relying Party's EU Business Wallet.
7. The Relying Party's EU Business Wallet validates the credential and its revocation status.
8. The Relying Party's EU Business Wallet sends the result to the Relying Party.
9. The Relying Party displays the result to the user.
- 10.

2.4 Scenario additional flows

A scenario may include certain variations of the main flow execution that the use case wants to pilot cross border. Like same device vs cross device execution.

A scenario may also want to address certain exceptions to the main basic flow. Like a user not having the proper mandate, diplomas, IBAN etc.

These can be mentioned in the table below, but only those that the use case really aims to pilot (so not every thinkable exception needs to be mentioned here, if the use case will not pilot that anyway. These may include several technical exceptions that need to be tested, but not explicitly piloted: these do not need to be included in the table below).

Flow	Short description
Variations	
Alternate issuance flow	Instead of having a presentation of the EBWOID followed by the issuance, the Issuer starts an "issuance with presentation" flow, requesting the EBWOID during the issuance process.
Revocation flow	After the Business Registry (Authentic Source), updates the information regarding the user and their capabilities to act as an appointed representative of the company, the Issuer (QTSP) of the attestation revokes it.
Presentation flow	The user tries to gain access to a service that requires a valid "PoR" attestation. The attestation is valid and not revoked, granting the user access to the service.
Exceptions	
Presentation flow	The user tries to gain access to a service that requires a valid "PoR" attestation. The "PoR" attestation has been revoked by the Issuer (QTSP) and as such, he is not granted access.
Issuance without representation	The user tries to initiate a "PoR" issuance in a scenario where he doesn't have the necessary powers. During the issuance process of a "PoR" attestation, the Authentic Source (Business Registry) determines that the requester does not have the claimed

powers	representation powers. As a result, the Issuer (QTSP) denies the issuance and the process is not completed
--------	--

If helpful, it can be made explicit what will NOT be piloted cross border. This should be in line with section 1.4 of the Stock Taking document.

2.5 Challenges and barriers

Describe the main challenges and barriers that are expected concerning the development of the solution needed for piloting the scenario. You can use the Stock Taking document sections 1.7, 4.2, 5, and 6 as a basis.

We can identify several challenges and barriers that may affect the successful implementation of this scenario:

Technical challenges:

- Interoperability between wallet providers, in particular between solutions from different wallet providers, where issuers and relying parties must support credentials presented from multiple wallets
- Integration between the authentic source and wallet providers or QTSPs, including integration with legacy systems of the authentic sources and wallet providers, and how data is made available (e.g. via APIs/connectors) to be consumed by the ecosystem

2.6 Working Assumptions

In case of significant uncertainties, working assumptions can be installed to establish ‘a stable foundation’ for the development of the scenario. The uncertainty may relate to (project) internal or external aspects, like the (future) availability of guidance on certain aspects in the ARF. In this case, the scenario may choose a direction for development, that is expected to be chosen in a future ARF as well.

3 Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

--	--	--	--	--

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exception
User authentication at QTSP	User	The user authenticates against the Issuer Service using an accepted authentication mechanism, such as a certificate, or equivalent national method.	Availability of a valid user authentication method accepted by the Issuer Service.	Authentication may fail due to invalid credentials, expired certificate, or unavailable authentication service.
Authentication result returned	Issuer Service / QTSP	The Issuer Service confirms that the user has been successfully authenticated and is authorised to continue the process.	The Issuer Service confirms that the user has been successfully authenticated and is authorised to continue the process.	If authentication is not successful, the process stops and the user is informed.
Request for PoR	User	After authentication, the user explicitly requests the issuance of a Power of	Successful user authentication.	The user may cancel the process before submitting the request.

		Representation (PoR).		
Request for EBWOID presentation flow	Issuer Service / QTSP	The Issuer Service requests the Issuer's EU Business Wallet to initiate the EBWOID retrieval flow.	User request for PoR has been received.	In an alternat flow, the issu may start the PoR issuance directly and request the EBWOID late within the sa flow.
QR code / link generation for EBWOID presentation	Issuer's EU Business Wallet	The Issuer's EU Business Wallet generates and returns a QR code or deeplink so that the user can start the presentation flow from the Company EU Business Wallet.	Issuer's EU Business Wallet must support OpenID4VP initiation.	If the QR cod or link canno be generatec the process cannot continue.
Presentation process started by user	User / Company EU Business Wallet	The user starts the presentation flow by scanning the QR code or activating the link with the Company's EU Business Wallet.	User has access to the Company's EU Business Walletand the QR code / link is valid.	Cross-device and same-device initiat are both possible, depending on pilot implementati
		The user		

User consent to share EBWOID	User / Company's EU Business Wallet	consents to present the EBWOID to the issuer side. This triggers the OpenID4VP presentation flow.	EBWOID must be available in the Company's EU Business Wallet. User consent is required.	The user may refuse consent in which case the process ends.
EBWOID sent to issuer side	Company's EU Business Wallet	The Company's EU Business Wallet sends the EBWOID attestation to the Issuer's EU Business Wallet	Issuer's EU Business Wallet. Successful OpenID4VP exchange and user consent	Transmission may fail due to technical issues or session timeout.
Validation of EBWOID	Issuer's EU Business Wallet	The Issuer's EU Business Wallet validates the attestation, including integrity, authenticity, and revocation status.	Receipt of a valid EBWOID presentation. Access to revocation and validation mechanisms.	Validation may fail if the attestation is expired, revoked, malformed, or not trusted.
Validation result sent to issuer service	Issuer's EU Business Wallet	The validation result and the attestation are transmitted to the Issuer Service / QTSP for the business verification step.	Successful attestation validation.	If validation fails, a negative result is sent and the process stops.
		The Issuer		

Verification of representation rights	Issuer Service / QTSP	Service queries the Business Registry / Authentic Source to verify whether the authenticated natural person is entitled to represent the relevant legal entity.	Availability of personal data, EBWOLD data, and connectivity to the Authentic Source.	The registry may return no match, partial match, or a negative confirmation
Representation status confirmed	Business Registry / Authentic Source	The Authentic Source confirms that the user has valid representation rights for the relevant company.	Successful query from the Issuer Service and authoritative data availability.	If representation rights are not confirmed, the PoR cannot be issued.
Request for PoR issuance	Issuer Service / QTSP	Once the representation rights are confirmed, the Issuer Service requests the Issuer's EU Business Wallet to initiate issuance of the PoR attestation.	Successful verification from the Authentic Source.	If the verification is negative, issuance is denied.
QR code / link generation for	Issuer's EU Business	The Issuer's EU Business Wallet creates a QR code or link	Issuance request from the Issuer Service.	In the alternative flow, this issuance flow may

	issuance	Wallet	to start the credential issuance flow.	Support for OpenID4VC issuance.	already have been initiated earlier.
	Issuance process started by user	User / Company's EU Business Wallet	The user starts the credential issuance flow from the Company's EU Business Wallet.	User has access to the Company's European Business Wallet and the QR code / link remains valid.	The user may abandon the process before accepting issuance.
	User consent to retrieve PoR	User / Company's EU Business Wallet	The user accepts receiving the PoR credential in the Company's EU Business Wallet. This triggers the OpenID4VC issuance flow.	User consent and a supported issuance flow.	The user may decline the credential issuance.
	Retrieval request for PoR attestation	Company's EU Business Wallet	The wallet requests the issuance and retrieval of the PoR attestation from the Issuer's EU Business Wallet.	Active OpenID4VC session and user acceptance.	Technical issues may interrupt the credential retrieval process.
	Representation	Issuer's EU Business	The Issuer's EU Business Wallet collects the relevant representation	Access to authoritative representation	Missing or inconsistent

data gathered	Wallet/ Business Registry	data from the Authentic Source in order to build the PoR credential.	data and positive issuance authorisation.	registry data may prevent issuance.
PoR attestation generated	Issuer's EU Business Wallet	The Issuer's EU Business Wallet generates the PoR attestation according to the applicable credential schema and trust framework.	Availability of verified representation data and issuance authorisation.	Credential generation may fail due to schema, signing, or system issue
PoR stored in wallet	Company's EU Business Wallet	The generated PoR attestation is delivered to and stored in the Company's EU Business Wallet.	Successful issuance and wallet support for storage of the credential.	Storage may fail if the wallet is full, incompatible or the transfer is interrupted
Success message shown	Company's EU Business Wallet/ User	The wallet informs the user that the PoR credential has been successfully issued and stored.	Credential issuance and storage completed successfully.	If any previous step failed, an error message is shown instead of a success message.

Alternative issuance method

In the alternative issuance method, the issuance flow is initiated first and the EBWOID presentation is requested as part of the same issuance interaction. Functionally, the verification and issuance outcome remain the same, but the order of interactions is different.

Revocation

If the user’s representation status changes in the Authentic Source after issuance, the QTSP may be notified or may detect the change. The QTSP then starts the revocation process and the Issuer’s EU Business Wallet revokes the previously issued PoR credential.

Presentation to a relying party

After issuance, the PoR can be presented by the user to a relying party through an OpenID4VP presentation flow. The relying party validates the credential and its revocation status before granting or denying access to the requested service.

4 Roles and participants

4.1 Scenario roles and participants

...

Describe the roles relevant for this scenario, and list which of the partners will play this role in piloting the scenario. Note that the roles primarily active in the use case are mentioned. Section 1.5 of the Stock Taking document can be used as a basis.

Primary role	UC partner Name	Country
1. User of EUDI/EUBW Wallet	Person with Powers of Representation (PoR) acting on behalf of a company e.g. while entering a Point of Sale and presenting needed information like Metadata, VAT-ID,elInvoice routing information (Person at a SME or Soletrader) or who will act with PoR towards an authority like dutch tax administration	DE / NL /SE

2. Authentic sources	Organisations which issue needed information e.g. PID, LPID, VAT-ID, PoR-attestation (for pilot e.g. by DATEV for person working on behalf of a SME or dutch tax administration/swedish tax authority to know the person who declares something with PoR towards them)	DE / NL / SE
3. Relying party	organization which refers to that needed information (for pilot e.g. BOSCH or the dutch tax administration, Skattverket), which needs the information to get a proper business process	DE / NL / SE
4. Intermediary		

4.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUBW Wallet provider	PROCIVIS CREDENCO SIROS iGrant	DE NL	
2. PID Provider	BDR Bolagsverket	DE SE	
3. Trusted list registrar	IDunion	DE	
4. QEAA provider	Registradores T-Systems / DTAG	ES DE DE	

	Cleverbase	FR	
	Docaposte	FR	
	Intesi	IT	
5. Pub-EAA provider		DE	
6. EAA provider	Registradores	ES	
	T-Systems / DTAG	DE	
	DATEV	DE	
	Cleverbase	FR	
	Docaposte	FR	
	Intesi	IT	
7. QES provider			

Land	Relying Party	Ctry	Issuer	Ctry	Name	Role
ES	Colegio de Registradores de España		Colegio de Registradores de España	PoA, PoR		
DE	Telekom	DE		PoA, PoR		
DE	DATEV eG	DE	DATEV eG	PoA, PoR		
FR	Docaposte			PoA, PoR		
IT	InfoCamere SCpA			PoA, PoR	InfoCamere SCpA	Wallet Provider

FR	Infogreffe			PoA, PoR		
ES				PoA, PoR	IZERTIS	Wallet Provider
BE	OpenPeppol AISBL			PoA, PoR	Orange	Wallet Provider
SE	Skattverket	SE	Skattverket	PoA, PoR		
DE					IDunion SCE	TrustList
					PagoPA	Wallet Provider
GR	GRNET	GR	GRNET	PoA, PoR	GRNET	Wallet Provider

4.3 Target country combinations

Because WE BUILD is a cross-border pilot but not all countries may want to pilot with all other countries, state which countries intend to pilot the scenario with each other.

	Issuing country						
		ES	NL	DE	ES	FR	SE
Relying Party country	AT			X			
	BE						
	DE	X	X	X	X		X
	NL	X			X		
	FR						
	SE						X

4.4 Requirements

The main requirements for each of the roles involved are included as an Annex.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Declare which attestations will be used in the scenario, but will NOT be designed, implemented and issued to wallet within the scenario

Attestation name	Short description	To be provided by	For Countries	Requirements
EBWOID (LPID)	Identification of the Legal Person	XX	All	The EBWOID should contain the necessary information to be able to verify it with the Business Registry.

5.3 Created attestations in the scenario

Describe the attestations what will be created by issuers, within the scenario (so these are not the 'foreign' attestations).

Note that for each of the attestations, a rulebook must be made during the specification phase.

- Each rulebook will be made in collaboration with the SEMANTICS workgroup from WP4. An example rulebook is provided, of which the Use Case shall create sections 1, 2 and 3 while WP4 SEMANTICS creates the sections 4 and onwards.
- We aim for fit-for-pilot attestations. Each rulebook describes the set of attestations the as agreed upon by the scenario partners from the perspective of requesting and providing, that are relevant for piloting the scenario. The rulebook shall not include attributes that either none of the relying parties need, or none of the issuers can provide for piloting the scenario, unless existing domain-standards that are adopted, dictate otherwise.

State which countries will create these attestations and ensure that this is aligned with the targeted country combinations in section 4.4 of this document.

Attestation name	Short description	For Countries	Applicable domain standards
Power of Representation (PoR)	Attestation describing representation powers of a Natural Person acting on behalf of a company	All	eIDAS EAA, Verifiable Credentials

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUDI Wallet	a. The EUDI Wallet maybe used in this pilot, but main focus will be on Business Wallets.
	b.

		c.
2. Authentic sources	a.	Must provide authoritative and up-to-date data regarding company registration and representation rights.
	b.	Must support secure interfaces (APIs or equivalent) to allow querying of representation data by QTSPs or EAA providers.
	c.	Must ensure data integrity, availability and legal reliability in accordance with national and EU regulations.
3. Relying party	a.	Must be able to request, receive and process verifiable credentials (PoR) via OpenID4VP flows.
	b.	Must validate credentials (authenticity, integrity, issuer trust, revocation status) either directly or via a trusted intermediary.
	c.	Must implement business logic to evaluate representation rights and decide whether to allow the requested corporate action.
4. Intermediary	a.	There are no intermediaries
	b.	
	c.	
5. European Business Wallet provider	a.	Must implement support for OpenID4VP and OpenID4VC flows, including secure credential storage and presentation.
	b.	Must ensure user control and consent over credential sharing.
	c.	Must support secure key management and comply with ARF and WP4 technical specifications.
6. PID Provider	a.	Might be used in this pilot
	b.	
	c.	

7. Trusted list registrar	a. Must ensure that relying parties and wallets can verify issuer trust status.
	b. Must keep trust lists updated and accessible in a standardized format.
	c.
8. Issuer Service	a. Must orchestrate the PoR issuance process, including authentication, request handling and interaction with wallets.
	b. Must query the Authentic Source to verify representation rights based on EBWOID and user identity data.
	c. Must trigger the issuance of the PoR attestation by the QEAA (QTSP) provider and ensure correct linkage to the user and legal entity.
9. QEAA (QTSP) provider	a. Must issue qualified electronic attestations of attributes in compliance with eIDAS2.
	b. Must ensure secure issuance processes and strong identity binding.
	c. Must support validation services including revocation status and trust verification.
10. PubEAA provider	a. Might be used inside this pilot
	b.
	c.
11. EAA provider	a. Might be used inside this pilot
	b.
	c.
12. QES provider	a. Not used inside this pilot

	b.
	c.

webuild-consortium / BU4

Type to search

Code

Issues

Pull requests2

Agents

Actions

Projects

Security and quality

BU4 / scenarios / 1C-Service-Access



borislingl

Change wallet provider from Bolagsverket to Skattverket

a17c932 · last month

History

Name	Name	Last commit date
..		
README.md	Change wallet provider fro...	last month

README.md

Scenario 1C — Get Access to a Service

MVP Scenario



WE BUILD

CONSORTIUM

Specification Scenario BU4 1c – Get access to service

WP2 – UC BU4 1c – Get access to service

Date : 19/06/2026

Version : 1.0 (<0.1 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)

Status : Final (Draft, for review, reviewed, final)

Index

1 Introduction

1.1 Objectives of this document

1.2 Scenario introduction

2 Scenario specification

2.1 Introduction

2.2 Scenario pre-conditions

2.3 Scenario main flow

2.4 Scenario additional flows

2.5 Challenges and barriers

2.6 Working Assumptions

3 Detailed scenario flow

4 Roles and participants

4.1 Scenario roles and participants

4.2 Additional roles and partners

4.3 Target country combinations

4.4 Requirements

5 Attestations

5.1 Introduction

5.2 Attestations to be provided by other UCs/WGs/scenarios

5.3 Created attestations in the scenario

Annex 1 – Requirements for scenario roles

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario **"Get access to service"**, as part of the use case "Company representative acting on behalf of company" [BU4] in work package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

Explain the scenario in one line, describing what will be piloted cross border.

A natural person uses a Business Wallet or a EUDI Wallet containing Power of Representation (PoR) and/or Power of Attorney (PoA) and/or Power of Employee (PoE) attestations to prove authorization to act on behalf of a legal entity and access digital services provided by cross-border public or private relying parties.

The scenario is based on the following documentation:

- Include references to ARF version
- Include references to Stock Taking document
<https://portal.webuildconsortium.eu/group/bu4-company-representative-acting-behalf-company/files?mid=5839&fid%5B0%5D=88&fid%5B1%5D=89&fid%5B2%5D=4194>

- Include references to relevant WP4 documentation
- Include references to relevant 1st generation documentation
- Include references to relevant domain documentation <https://github.com/webuild-consortium/wp4-architecture/tree/main/adr>

2 Scenario specification

2.1 Introduction

Provide a high level introduction of the scenario. Possibly copy-paste this from the Stock Taking document.

Declare under which UC this scenario resides and if the scenario is part of the MVP or MVP+.

Declare if the scenario will use a Natural Person Wallet, a legal Person Wallet or both.

Get access to service scenario: Use of PoX (PoA and/or PoR and/or PoE) attestations for access to commerce platforms, public platforms, get payment or balance sheets at banks and other situations that require representation of companies.

This scenario is part of the MVP scope of BU4 and focuses on the use of representation credentials for accessing cross-border services.

2.2 Scenario pre-conditions

Detail the relevant pre-conditions from the Stock Taking document, section 1.6.

For the Use Case to succeed there are several conditions that have to be met on top of the ones that have to be developed in the Use Case itself:

- Availability of an EBW that incorporates the EBWOID of the company involved in the cross-border operation;
- KYC / KYS scenarios are finalized (from BU1)

- Availability of an EUDIW that incorporates the PID of the person acting on behalf of the company;
- Availability of the EU Company Certificate in the EBW;
- Capability of QTSPs to issue PoX attestations (PoA, PoR) as QEAA, with a clearly defined issuance process (required inputs, verification steps, supporting documents such as PID, EU Company Certificate, company statutes, etc.) ; or capability of a company to issue a PoE (Power of Employee) as EAA.

PoX origin variants covered by this scenario

The PoX attestation presented in this scenario may originate from different contexts:

- PoA / PoR issued by a QTSP as a QEAA, based on:
 - i. authentic source information (e.g. business register, ...), or
 - ii. a rulebook/process and expression of will of the represented party (not necessarily backed by an authentic source).
- PoE issued by a company as EAA.

The PoX attestations may be delivered to different recipients:

- PoA / PoR / PoE stored in the EUDIW of the natural person;
- PoA stored in the EBW of an organization

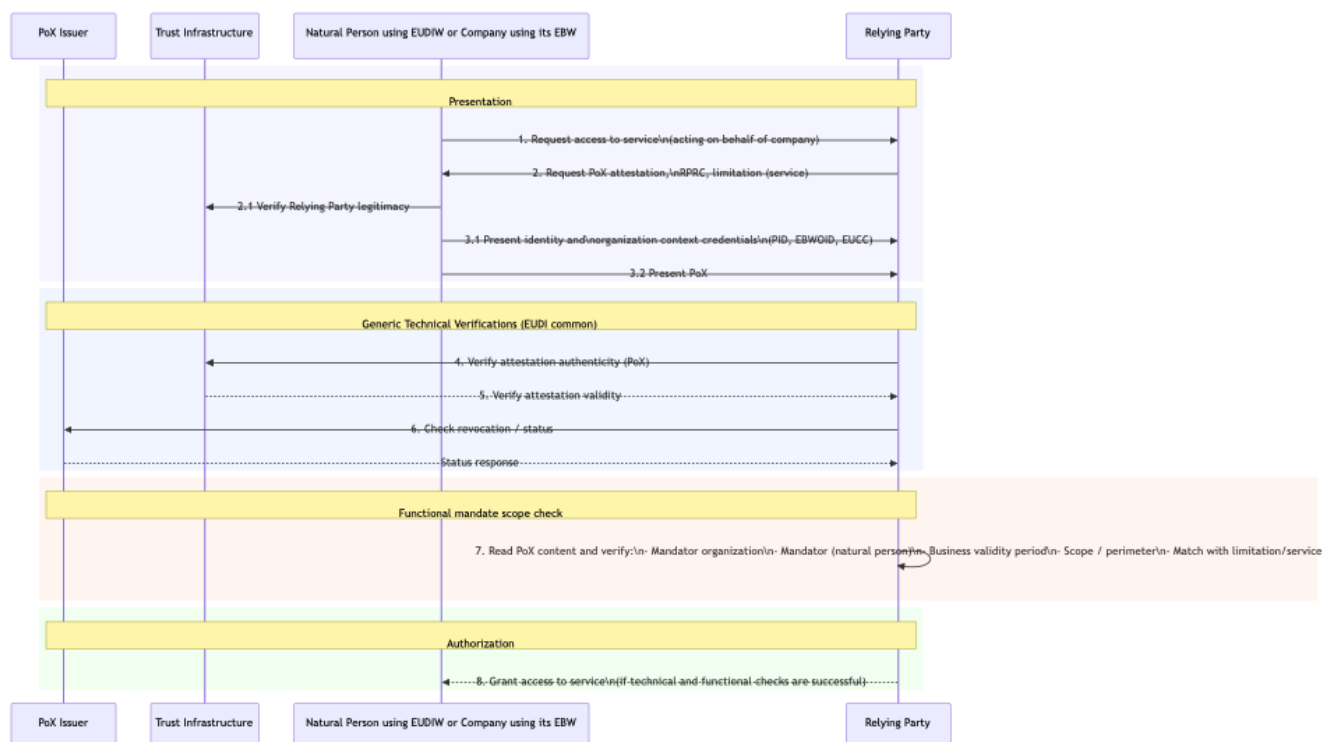
In all these cases, the presentation and verification flow at the Relying Party remains identical, as described in the swimlane diagram below.

2.3 Scenario main flow

Provide a swimming lane diagram of the one main process flow that will be piloted cross border, to mark the beginning, ending and most important steps. Constrain to the following swimming lanes : User (incl wallet), Relying Party (may be split into intermediary and relying party), (Q)EAA or Public-EAA provider, QES provider, (L)PID provider.

Note: This swimlane diagram illustrates the nominal flow, assuming that all verification steps are successful and no validation fails.

Referemce to Swimlane in Github: https://github.com/webuild-consortium/BU4/blob/main/scenarios/diagrams/1c_fow.mmd



2.4 Scenario additional flows

A scenario may include certain variations of the main flow execution that the use case wants to pilot cross border. Like same device vs cross device execution.

A scenario may also want to address certain exceptions to the main basic flow. Like a user not having the proper mandate, diplomas, IBAN etc.

These can be mentioned in the table below, but only those that the use case really aims to pilot (so not every thinkable exception needs to be mentioned here, if the use case will not pilot that anyway. These may include several technical exceptions that need to be tested, but not explicitly piloted: these do not need to be included in the table below).

Flow	Short description
Variations	
Required QES (service-dependent)	The service requires a Qualified Electronic Signature (QES) to complete the access process,

	depending on the service trust level and legal requirements.
Access via RP intermediary (platform/marketplace)	The user accesses the service through an intermediary Relying Party (e.g., marketplace or platform acting on behalf of the final service provider), which orchestrates the access request and authentication flow.
Same-device vs cross-device execution	The access flow is executed either on a single device (end-to-end) or across multiple devices (e.g., initiation on desktop and completion on mobile), depending on user context and available wallets.
Exceptions	
PoX scope does not match requested service	The mandate presented in the PoX does not cover the service the user is trying to access.
PoX validity period expired	The mandate is technically valid but outside of its business validity period.
PoX revoked	The revocation/status check returns that the mandate is no longer valid.
Trust chain / signature verification failure	The RP cannot validate the signature or the trust chain of the PoX issuer.
Identity mismatch with PoX	The natural person presenting the wallet is not the one identified in the PoX as the mandatory.
Required QES not provided	The service requires a Qualified Electronic Signature but the user provides a lower-level

	signature.
• Cross-border trust recognition failure	(For PoA and PoR only) The QTSP issuing the PoA/PoR is not recognized or trusted by the Relying Party jurisdiction.

If helpful, it can be made explicit what will NOT be piloted cross border. This should be in line with section 1.4 of the Stock Taking document.

This Use Case will not consider any of the following situations or areas:

- Mandates that cannot be cryptographically or organizationally bound to an identified legal entity (EBWID) and verified through the EU Company Certificate (EUCC)
- Mandates that are not based on European Regulation or a Member State national regulation (e.g. mandates based on the role within the company such as purchasing capabilities for the CFO).

2.5 Challenges and barriers

Describe the main challenges and barriers that are expected concerning the development of the solution needed for piloting the scenario. You can use the Stock Taking document sections 1.7, 4.2, 5, and 6 as a basis.

Challenge / Barrier	Description
Heterogeneity of mandate models across Member States	Mandates (PoA/PoR) are defined and managed differently in each country, making cross-border interpretation by the RP difficult.
Lack of harmonization of attestations and authentic sources	No common structure or semantics yet for PoA/PoR and authentic source data across Member States.
Cross-border trust recognition	A PoX technically valid in one country may not be recognized or trusted by an RP in another country.
Dependency on evolving standards	Some required standards are still in draft, which may

(e.g. ETSI TS 119 478)	require adjustments during the pilot.
Dependency on Wallet and QTSP capabilities (WP4)	The scenario relies on external wallet and signature capabilities not controlled by the use case.
Availability of business registers and authentic sources	Limited access, APIs, or digitization of registers may prevent proper mandate validation.
Regulatory evolution during the project	New or clarified Implementing Acts may impact how the scenario must be implemented.
Complexity of cross-border corporate representation	Legal and operational differences make corporate mandate verification complex across borders.
Semantic alignment between actors	Misalignment on the meaning/structure of mandate attributes may lead to valid PoX being rejected.

2.6 Working Assumptions

In case of significant uncertainties, working assumptions can be installed to establish 'a stable foundation' for the development of the scenario. The uncertainty may relate to (project) internal or external aspects, like the (future) availability of guidance on certain aspects in the ARF. In this case, the scenario may choose a direction for development, that is expected to be chosen in a future ARF as well.

Assumptions	Description
Common PoX structure usable cross-border	A PoX containing PoA/PoR information can be interpreted by RPs in other Member States.
Machine-readable access to authentic	Business registers and mandate sources will be accessible through interfaces usable by RPs.

sources	
Cross-border trust chain verification	RPs will be able to verify the trust chain of foreign PoX issuers using eIDAS mechanisms.
Wallet support for PoX presentation and QES	Wallets will support PoX presentation and qualified signatures when required by the service.
Minimal semantic alignment on mandate attributes	A shared understanding of mandate attributes (role, scope, validity) will exist across actors.
Reliance on current ARF scope	The scenario is developed based on the current ARF and not on future EU Business Wallet specifications.
Pre-agreed semantic model for PoE interpretation	For PoE, the meaning of role and scope attributes cannot be interpreted generically cross-border and must rely on a semantic model previously agreed between the Relying Party and the organization issuing the PoE.

3 Detailed scenario flow

Per step in the main flow, a detailed description is made in the table below.

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions

1. Request access to service	Natural Person using EUDIW	User navigates to the service website and selects "Access on behalf of a company".	/	Same vs Cross device variation applies
	Relying Party	RP detects that access is requested in a representative capacity and prepares a PoX request.	PoX model	Access via RP intermediary variation
2. Request PoX attestation	Relying Party	RP sends a request to the wallet specifying required PoX attributes, RP purpose and service limitation.	PoX / PoA / PoR / PoE structure from mandate UC	Required QES variation: if a QES is required by the service, the RP may rely on the identity contained in the QES certificate and not require the PID to be presented separately.
	Natural Person using EUDIW	Wallet receives the request and displays requested attributes to the user for consent.	Wallet capabilities (WP4)	/

3. Share PoX	Natural Person using EUDIW	User consents and wallet prepares the PoX presentation including required attestations.	PoX issued from authentic source UC	Required QES exception if missing
	Natural Person using EUDIW	Wallet sends PoX presentation to RP.	Wallet presentation flow (WP4)	Same vs Cross device variation
	Relying Party	RP receives PoX and initiates verification process.		
4. Verify signature	Relying Party	RP verifies the signature of the PoX against the identity of its issuer: via the EU Trusted List for PoA/PoR issued by QTSPs, or against the organization identity (EBWOID/EUCC) for PoE issued by an EAA.	QTSP / Trust list UC	Cross-border trust exception
5. Verify trust chain	Relying Party	RP validates issuer trust chain.	eIDAS trust framework	Cross-border trust exception
6. Verify technical		RP checks		Expired PoX

validity dates	Relying Party	attestation validity period.	PoX metadata	exception
7. Check revocation / status	Relying Party	RP queries status/revocation infrastructure for mandate validity.	Authentic source / status UC	PoX revoked exception
8. Return current status	Status infrastructure	Status service returns current validity (valid/revoked).	Authentic source UC	/
9. Read PoX content	Relying Party	RP extracts mandator organization and mandatory identity from PoX.	PoX semantic model UC	Identity mismatch exception
	Relying Party	RP checks business validity period of the mandate.	PoA/PoR model UC	Expired mandate exception
	Relying Party	RP verifies scope/perimeter of mandate matches requested service.	Mandate scope model UC	Scope mismatch exception
10. Grant access	Relying Party	RP grants access to the service on behalf of the company after successful checks.		

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of EUDI Wallet	End users (citizens and businesses) accessing services via the EUDI and European Business Wallet in the context of cross-border public/private service access	EU (multi-country)
2. Authentic sources	IDunion SCD (trust list)	GE
3. Relying party	OpenPeppol AISBL	BE
	Itsme	BE
	Skatteverket	SE
	DATEV	DE
	GRNET	GR
	Orange Business (for PoE) [TBC]	FR
4. Intermediary		

4.2 Additional roles and partners

Describe which partners that primarily work in WP4 participate in piloting this scenario. Section 3 from the Stock Taking document can be used as a basis.

There are several dependencies with other working packages, all of them lie within the WP4 General capabilities. The description and severity of the dependencies are as follows:

- **Semantics Group.** The semantics group establishes a moderate dependency, in that although it is desirable for the definition of terms to be agreed upon throughout the consortium through this group, one could choose to create one's own definitions within the use case to avoid deadlocks and allow for the continuity of the use case.
- **PID&LPID Provider.** This group establishes a strong dependency, as it is necessary to have the company identifiers (LPID) and its representative (PID) to be able to carry out any transaction in the EU cross-border context.
- **QTSP (incl. Signatures) and Organization issuers (EAA).** This dependency is necessary for PoA/PoR issued as QEAA by QTSPs, and for PoE issued directly by organizations acting as EAA. Both types of issuers produce PoX attestations that must be verifiable and usable by the wallets and Relying Parties.
- **Wallet providers.** The WP4 working group is presented as a necessary dependency as they are the providers of the cross-functional technology that will enable the end-to-end execution of use cases.
- **EUBW draft, further enhancements of the upcoming EUBW regulation and its implementation to national law**

Primary role	UC partner Name	Country	Wallet
1. EUBW Wallet provider	PROCIVIS	DE	
	CREDENCO	NL	
2. PID Provider	BDR	DE	
3. Trusted list registrar	IDunion	DE	
	Registradores	ES DE	

4. QEAA provider	T-Systems / DTAG	DE	
	Cleverbase	FR	
	Docaposte	FR	
	Intesi	IT	
5. Pub-EAA provider			
6. EAA provider	Registradores	ES	
	T-Systems / DTAG	DE	
	DATEV	DE	
	Cleverbase	FR	
	Docaposte	FR	
	Intesi	IT	
7. QES provider			

RP Country	RP Name	Issuer Country	Issuer Name	Attestation	Name	F
DE	DATEV eG	DE	DATEV eG	PoA, PoR		
NL	Belastingdienst		BU3	PoA, PoR		
DE					IDunion SCE	Tru
BE	OpenPeppol AISBL			PoA, PoR		
BE	Itsme					
						Wæ

FR	Orange				Orange	Prø
SE	Skattverket				PagoPA	Wæ Prø
GR	GRNET	GR	GRNET	PoA, PoR	GRNET	Wæ Prø

4.3 Target country combinations

Because WE BUILD is a cross-border pilot but not all countries may want to pilot with all other countries, state which countries intend to pilot the scenario with each other.

	Issuing country						
		ES	NL	DE	ES	FR	...
Relying Party country	AT			X			
	BE						
	DE	X	X	X	X		
	NL	X			X		
	FR						

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex 1.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Declare which attestations will be used in the scenario, but will NOT be designed, implemented and issued to wallet within the scenario

Attestation name	Short description	To be provided by	For Countries	Requirements
Person Identification Data (PID)	Verifiable identification of the natural person using the wallet, enabling the Relying Party to uniquely identify the representative presenting the PoX attestation	<i>UC/WG responsible for PID issuance within WeBuild</i>	FR, DE, IT, ES, BE, SE, GR, NL	MUST allow unique identification of the natural person acting on behalf of a legal entity. MUST be issuable to the EUDI Wallets used in this scenario. MUST be verifiable by all Relying Parties involved.
Legal	Verifiable identification of the legal			MUST allow the Relying Party to verify the existence and identity of the legal entity

Person Identification Data (LPID) / Legal Entity Attestation	entity referenced in the PoX attestation, based on official business register data	<i>UC/WG responsible for Legal Entity / Business Register attestations</i>	FR, DE, IT, ES, BE, SE, GR, NL	referenced in the PoX. MUST be based on authentic sources (business registers). MUST be verifiable across borders.
Qualified Electronic Attestation / Qualified Certificate for signature validation	Qualified trust evidence allowing the Relying Party to verify the signature of the PoX attestation issuer and validate the trust chain	<i>WG dealing with Trust Services / eIDAS trust framework integration</i>	EU	MUST allow verification of issuer signature through QTSP certificates. MUST be discoverable through EU Trusted Lists. MUST support trust chain validation by the Relying Party.
Credential Status / Revocation	Mechanism allowing the Relying Party to verify whether the PoX	<i>WG dealing with Status/Revocation infrastructure</i>	EU	MUST allow real-time or near real-time status verification of the PoX attestation. MUST be accessible by

Information	attestation is still valid or has been revoked			all Relying Parties. MUST integrate with wallet and trust verification flow.
-------------	--	--	--	--

5.3 Created attestations in the scenario

Describe the attestations what will be created by issuers, within the scenario (so these are not the 'foreign' attestations).

Note that for each of the attestations, a rulebook must be made during the specification phase.

- Each rulebook will be made in collaboration with the SEMANTICS workgroup from WP4. An example rulebook is provided, of which the Use Case shall create sections 1, 2 and 3 while WP4 SEMANTICS creates the sections 4 and onwards.
- We aim for fit-for-pilot attestations. Each rulebook describes the set of attestations the as agreed upon by the scenario partners from the perspective of requesting and providing, that are relevant for piloting the scenario. The rulebook shall not include attributes that either none of the relying parties need, or none of the issuers can provide for piloting the scenario, unless existing domain-standards that are adopted, dictate otherwise.

State which countries will create these attestations and ensure that this is aligned with the targeted country combinations in section 4.4 of this document.

Attestation name	Short description	For Countries	Applicable domain standards
	Verifiable credential attesting that		Verifiable Credentials Data Model v2.0; SD-

Power of X (PoX) – Representation and Mandate Attestation (PoR + PoA + scope limitation)	a natural or legal person is empowered to act on behalf of a legal entity, including the role (PoR) or delegated mandate (PoA), the scope of powers, validity period, and service limitation. The attestation is based on authentic sources (business registers) and designed for selective disclosure and cross-border interoperability in EUDI Wallets.	FR, DE, IT, ES, BE, SE, GR, NL	JWT VC; ETSI TS 119 471; ETSI TR 119 476; ETSI TS 119 412-6; RPAM Ontology (SEMIC); EUDI ARF Attestation Rulebook Template
Power of Employee (PoE) – Organizational Representation Attestation	Verifiable credential attesting that a natural person is empowered by a legal entity to act on its behalf based on an internal organizational decision (e.g. employment or delegated function). The attestation defines the role and scope of powers according to a model agreed between the organization and the Relying Party. The attestation is cryptographically bound to the organization identity (EBWID) and verifiable through the EU Company Certificate (EUCC), and designed for selective disclosure and use in EUDI Wallets.	FR, DE, IT, ES, BE, SE, GR, NL	Verifiable Credentials Data Model v2.0; SD-JWT VC; ETSI TS 119 471; RPAM Ontology (SEMIC); EUDI ARF Attestation Rulebook Template

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUDI Wallet	a. MUST be able to authenticate towards Relying Party using EUDI Wallet credentials (PID or equivalent)
	b. MUST be able to consent to selective disclosure of attributes before transmission
	c. SHOULD be able to review requested attributes before approval
	d. MUST receive confirmation of successful or failed authentication
	e. MUST be able to act on behalf of a legal person based on a valid mandate
2. Authentic sources	a. MUST provide validated attributes upon request from authorized Relying Parties
	b. MUST ensure data integrity, correctness and up-to-date status of attributes
	c. MUST respond within defined time constraints to attribute requests
	d. MUST only release data under legal and trust framework conditions

	3. Relying party	a. MUST request only minimum necessary attributes for service access (data minimisation)
		b. MUST verify authenticity and validity of received credentials
		c. MUST support EUDI Wallet-based authentication flow
		d. MUST verify mandate linking natural person to organization
	4. Intermediary	a. MUST ensure secure communication between Wallet, Relying Parties and Authentic Sources
		b. MUST ensure interoperability of identity and attribute exchange formats
		c. MUST enforce consent management mechanisms
		d. MUST ensure compliance with EUDI trust framework
	5. EUDI Wallet provider	a. MUST support issuance and storage of PID and/or attestations required in the scenario
		b. MUST ensure wallets issued in participating countries can be used across all Relying Parties in this scenario
		c. MUST support authentication and attribute presentation flows as required by Relying Parties

		d. MUST ensure secure storage and cryptographic protection of credentials
6. PID Provider		a. MUST provide PID issuance in participating Member States included in the scenario
		b. MUST ensure issued PID can be used across all participating EUDI Wallet Providers
		c. MUST support cross-border recognition of PID within EUDI framework
7. Trusted list registrar		a. MUST maintain up-to-date list of trusted entities (wallets, issuers, relying parties) used in the scenario
		b. MUST ensure availability of trust status information for validation of credentials
		c.
8. QEAA provider		a.
		b.
		c.
9. Pub-EAA provider		a.
		b.
		c.
		a.

10. EAA provider	b.
	c.
11. QES provider	a.
	b.
	c.

WE BUILD consortium

Specification Scenario 1 – Micro- credentials

WP2 – BU5 Issue Micro credentials

Date : 18 June 2026
Version : 1.0
Status : Draft

Index

1	Introduction	3
1.1	<i>Objectives of this document.....</i>	3
1.2	<i>Scenario introduction.....</i>	3
2	Scenario specification.....	5
2.1	<i>Introduction</i>	5
2.2	<i>Scenario pre-conditions</i>	5
2.3	<i>Scenario main flow</i>	8
2.4	<i>Scenario additional flows.....</i>	8
2.5	<i>Challenges and barriers</i>	8
2.6	<i>Working Assumptions</i>	9
3	Detailed scenario flow.....	11
4	Roles and participants	13
4.1	<i>Scenario roles and participants.....</i>	13
4.2	<i>Additional roles and partners</i>	13
4.3	<i>Target country combinations.....</i>	13
4.4	<i>Requirements.....</i>	14
5	Attestations	15
5.1	<i>Introduction</i>	15
5.2	<i>Attestations to be provided by other UCs/WGs/scenarios</i>	15
5.3	<i>Created attestations in the scenario</i>	15

16

Feil! Bokmerke er ikke definert.

1 Introduction

The purpose of this Use Case Specification document is to define a coherent scenario for the issuance, management, presentation, and verification of a Micro-credential attestation in the context of the European Digital Identity Wallet (EUDI Wallet) ecosystem and the WE BUILD large scale pilot. In this document, the Micro-credential attestation is treated as an Electronic Attestation of Attributes (EAA) within the meaning of the revised eIDAS framework. Under the European Digital Identity Regulation, EAAs are electronic attestations that allow attributes to be authenticated, and EUDI Wallet users must be able to request, receive, store, select, combine, present, and share such attestations through their wallet.

This specification is intended to describe the use case from an operational and interoperability perspective. It focuses on the business and trust interactions among the relevant actors, the functional steps of the scenario, the required attestations, and the main requirements that the scenario imposes on participating parties. The document is not a legal interpretation of the Regulation, but it is designed to be aligned with the concepts, roles, and capabilities established by the European Digital Identity framework and its implementing acts.

The scenario addresses a recurring need in cross-border and domestic digital interactions: enabling a natural person to prove formally taught knowledge, skills, and competences with clear academic provenance and portability. In practical terms, this means that a person should be able to receive a digitally issued attestation about skills or competences from a legitimate issuer, hold that attestation in an EUDI Wallet, and present it to a relying party when required for a service, procedure, or eligibility decision. The trust objective is not merely technical portability, but semantically and organisationally reliable attribute exchange with appropriate user control.

This chapter introduces the objectives and the basic scenario concept. The following chapters then define the scenario in greater detail, including pre-conditions, main and alternative flows, participating roles, requirements, and the attestations involved.

1.1 Objectives of this document

This document describes the details of scenario 1 Micro-credentials, as part of use case BU5 Issue Micro credentials in work package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

The scenario concerns a **Micro credential attestation** issued for a natural person and used through an EUDI Wallet. A natural person gets issued one or more micro-credential(s) in one country and use them to apply to a university course or program in another country,

demonstrating fulfillment of entry requirements or recognition of credits based on one or more micro-credential(s).

At a high level, the scenario proceeds as follows. A legitimate issuer prepares and issues a Micro credential attestation for a wallet user. The wallet user receives the attestation in the EUDI Wallet and retains control over whether, when, and to whom it is presented. When a relying party needs evidence of the relevant Micro credential attributes, the wallet user can present the attestation from the wallet. The relying party then verifies the attestation and uses the verified result in its own decision-making process, for example in relation to access to a service, eligibility for a study programme, enrolment, professional onboarding, or another formally taught knowledge dependent procedure. This interaction pattern is consistent with the role of the EUDI Wallet as a means for users to receive, store, and share electronic attestations of attributes in a trusted and interoperable manner.

This scenario is informed by relevant European and international reference frameworks for the representation, interoperability, and governance of skills- and learning-related information. These frameworks include:

- [WE BUILD BU5 Micro-credentials UC Scenario Specification](#)
- [WE BUILD BU5 Micro-credentials Attestation Design](#)
- [WE BUILD Architecture and integration blueprint](#)
- [WE BUILD PID Schema and issuance Rulebook](#)
- [ESCO \(European Skills, Competences, Qualifications and Occupations\)](#), as the European multilingual classification of skills, competences, qualifications and occupations;
- [the European Learning Model \(ELM\)](#), as a multilingual data model supporting the interoperable representation of learning opportunities, qualifications, accreditation and credentials, with implementation documentation available in the [ELM Browser](#);
- [the Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability \(2022/C 243/02\)](#), as a relevant policy reference for the description and recognition of smaller learning achievements;
- [the Dreyfus model of skill acquisition](#), as a conceptual reference for stages of competence development;
- [ISO 21001:2025 — Educational organizations — Management systems for educational organizations — Requirements with guidance for use](#), as a relevant organisational reference for management systems for educational organisations.
- [the DC4EU Business Blueprint \(BBP\)](#), as a relevant reference for business processes, governance, onboarding, and credential lifecycle design in EUDI Wallet-related deployment contexts; and
- the WE BUILD [BU5 Stock Taking Document](#).

2 Scenario specification

2.1 Introduction

Learning new skills -both on the job and in the classroom- must increasingly form a continuous part of people's professional lives to keep up with evolving economies and ensure lifelong learning. The Union of Skills initiative proposed by the European Commission intends to expand the use of micro-credentials as flexible learning solutions. The BU5 use case aligns with this initiative and with the European Council recommendation on Micro-credentials (2022), to bridge the gap between formal education and learning on the job. Developing and implementing tools that support transparent and robust certification of Skills and labour market experience, will pave the way for a verified CV, skills-based recruitment, and enhanced workforce mobility.

Micro-credential (formal education)

The European Council has specifically defined the micro-credential in a 2022 Council recommendation ([source](#)): It is a portable, learner-owned record of assessed learning outcomes from a small, coherent volume of study that is often delivered by a formal education provider (e.g., HEI or VET). It can be aligned to a curriculum, carries notional workload (often in ECTS) and a level/cycle reference (such as EQF/QF-EHEA), and is issued under institutional quality assurance. Outcomes are assessed against transparent criteria, and the credential may stand alone or stack toward larger awards. Its primary purpose is to recognise formally taught knowledge, skills, and competences with clear academic provenance and portability.

The micro-credential scenario is part of the MVP in BU5 and will be using the natural person wallet.

2.2 Scenario pre-conditions

Before the Micro-credential scenario can be executed, the following pre-conditions shall be met:

- 1. A legitimate use context exists.**
An educational context must exist in which proof of one or more learning outcomes is required to apply for a course at a university.
- 2. The attestation subject is identifiable and in scope.**
The subject of the attestation must be a natural person who can be linked to the claimed learning outcome in a sufficiently reliable manner and who is eligible to receive, hold, and present the attestation through an EUDI Wallet.
- 3. The user possesses an activated EUDI Wallet.**
The user must possess an activated and operational EUDI Wallet that is ready to receive, store, select, and present attestations in the context of the scenario.
- 4. A PID attestation, or (for piloting purposes) mock PID attestation, is available in the wallet.**
The user's wallet must already contain a Personal Identification Data (PID) attestation, or a mock PID attestation where the scenario is executed in a pilot, test, or controlled demonstration environment. This PID-based identification data must enable the issuer and, where applicable, the relying party to bind the Micro-credential attestation to the correct natural person.

5. **The wallet user can act under their own control.**
The scenario assumes that the wallet user is able to manage the receipt and presentation of the attestation under their own control, unless a specific representation model or legal mandate applies.
6. **A relevant learning outcome assessment has been successfully completed.**
The attestation subject must have successfully completed the relevant learning outcome assessment, evaluation, or validation process required for the micro-credential claim to be issued.
7. **The completed assessment is documented and available as evidence.**
The result of the completed learning outcome assessment must be available in a form that can serve as the basis for issuing the micro-credential attestation.
8. **A sufficient evidence base exists.**
The learning outcome claim must be supported by an evidence base that is sufficiently robust for the intended purpose of the attestation.
9. **The assessment conditions are sufficiently transparent.**
The conditions under which the micro-credential evidence was generated and assessed must be defined in a sufficiently transparent and consistent way to support trust in the attestation.
10. **An eligible issuer exists.**
An issuer must exist that is authorised, recognised, or otherwise accepted within the applicable governance framework to issue a micro-credential attestation for the relevant type of skill claim.
11. **The issuer can link the evidence to the attestation subject.**
The issuer must be able to establish a reliable association between the underlying evidence and the natural person to whom the attestation will be issued.
12. **The issuer has access to the underlying evidence.**
The issuer must have access to the evidence on which the attestation is based, either directly or through an authorised and reliable source.
13. **A common semantic basis exists.**
The skill information must be representable using a defined attribute set and a recognised semantic structure so that it can be interpreted consistently by different parties.
14. **A recognised taxonomy or classification can be used where applicable.**
Where relevant, the skill should be referable to a common taxonomy or classification, such as ESCO, in order to support semantic interoperability across organisational and cross-border contexts.
15. **An attestation model is available.**
A defined model for the micro-credential attestation must exist, including the minimum data elements, metadata, identifiers, and structural components required for issuance, wallet storage, presentation, and verification.
16. **Wallet functionality is available for the scenario.**
The wallet used in the scenario must be capable of receiving, storing, selecting, and presenting the micro-credential attestation in the applicable scenario context.
17. **Verification capability is available.**
The relying party must have the means to request, receive, and verify the attestation in accordance with the applicable trust and verification framework.

18. Trust conditions are in place.

The relying party must be able to assess whether the presented attestation is authentic, valid, and acceptable for the intended purpose. This presupposes that issuer trust, attestation status, and verification rules can be evaluated.

19. Organisational readiness exists.

The participating organisations must have sufficient clarity on their roles, responsibilities, and operational processes for issuing, holding, presenting, and verifying the attestation.

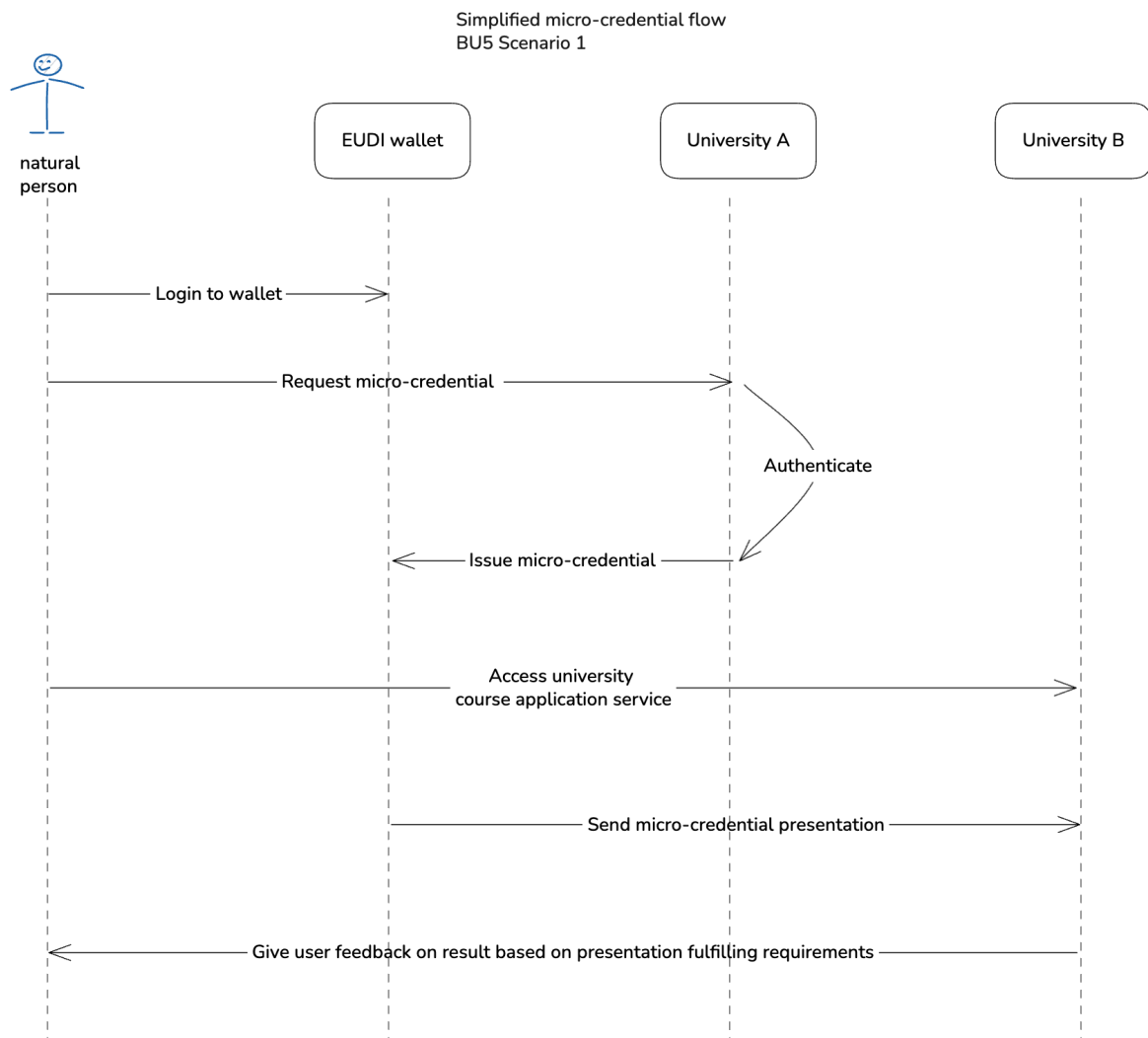
20. Legal readiness exists.

The participating parties must have an appropriate legal basis and sufficient legal clarity for processing the relevant data and for relying on the attestation in the intended context.

21. User-centred presentation is supported.

The scenario assumes that the attestation is presented by, or under the control of, the wallet user and that disclosure of skill-related information can be limited to what is necessary for the relying party's purpose, where supported by the applicable wallet and attestation model.

2.3 Scenario main flow



2.4 Scenario additional flows

No additional flows are planned to be piloted in the micro-credential MVP scenario.

2.5 Challenges and barriers

The technical standards used in the previous LSPs to achieve interoperability are already outdated and more recent drafts and versions of those standards exist. Many of the technical specifications used in the past are starting to reach a level of maturity where the updates are not as frequent. However, there are still changes and updates happening and this will be a mayor challenge in WE BUILD, as it was in the previous LSPs.

The higher education sector already is investing in micro-credentials formatted in JSON-LD according to the European Learning Model (ELM). This is currently not in line with the standards proposed for the EUDIW credential formats. BU5 goal is to find a way to pilot a micro-credential in line with the work already happening in the higher education sector but also aligned with the EUDIW standards and specifications.

2.6 Working Assumptions

In case of significant uncertainties, working assumptions can be installed to establish 'a stable foundation' for the development of the scenario. The uncertainty may relate to (project) internal or external aspects, like the (future) availability of guidance on certain aspects in the ARF. For the purpose of this Use Case Specification, the following working assumptions apply:

- a. **The Micro credential attestation is treated as an Electronic Attestation of Attributes (EAA).**
The scenario assumes that the Micro credential attestation is issued, held, presented, and verified within the EUDI Wallet ecosystem as a non-qualified EAA.
- b. **The scenario concerns formal-education skills and competences.**
The use case assumes that the Micro credential attestation concerns regulated skills but does not in itself grant a legal licence, regulated professional status, or formal right to practise.
- c. **The attestation subject is a natural person.**
The Micro credential attestation is assumed to relate to a natural person who is able to receive, hold, and present the attestation through an EUDI Wallet.
- d. **The wallet user has an activated wallet and a PID or mock PID attestation.**
The scenario assumes that the wallet user possesses an activated EUDI Wallet and that the wallet already contains a PID attestation, or a mock PID attestation in a pilot or test environment, enabling reliable identity linkage in the scenario.
- e. **A relevant skills assessment has been completed successfully.**
The scenario assumes that the attested skill is based on a completed assessment, evaluation, or validation process and that the result is available as documented evidence.
- f. **The issuer is eligible to issue the attestation.**
The scenario assumes that the issuer is authorised, recognised, or otherwise accepted within the applicable governance framework to issue the Micro credential attestation for the relevant type of skill claim.
- g. **Identity binding is performed at issuance.**
The scenario assumes that the issuer establishes a reliable binding between the attestation subject, the relevant identity information, and the supporting assessment evidence before issuing the attestation.
- h. **Holder authentication and authorisation are required at presentation.**
The scenario assumes that presentation of the Micro credential attestation takes place under the control of the wallet holder, who authenticates to the wallet and authorises disclosure in response to a relying party request.
- i. **The attestation model is aligned with the micro-credential model.**
The scenario assumes that the Micro credential attestation should remain within micro-credential structures to support recognition and interoperability.
- j. **A common semantic basis is available.**
The scenario assumes that the attested skill can be represented using a defined attribute set and a recognised semantic structure, and that a recognised taxonomy or classification, such as ESCO, can be used where applicable.
- k. **Selective disclosure should be supported where possible.**
The scenario assumes that, where supported by the wallet and attestation model,

the wallet user should be able to disclose only the subset of attested information necessary for the relying party's purpose.

l. The attestation may need lifecycle management.

The scenario assumes that a Micro credential attestation may require validity information, review dates, reassessment, renewal, replacement, suspension, or other lifecycle controls, depending on the nature of the skill and the applicable governance rules.

m. The scenario supports both domestic and cross-border use.

The scenario assumes that the Micro credential attestation may be used in both domestic and cross-border contexts, although semantic interpretation, policy alignment, and recognition may vary across sectors and jurisdictions.

Detailed semantic, governance, and conformance requirements are defined in the Rulebook.

This Use Case Specification assumes that the detailed requirements governing attestation content, issuance conditions, assurance levels, quality levels, lifecycle rules, and verification obligations will be defined in the Micro credential Attestation Rulebook.

3 Detailed scenario flow

The main flow of the micro credential scenario consists of the following steps:

1. **A need to demonstrate a learning outcome arises.**
A wallet user is required, or chooses, to prove possession of a specific learning outcome from an earlier learning achievement.
2. **The learning outcome has previously been assessed successfully.**
The wallet user has successfully completed the relevant learning achievement assessment, evaluation, or validation process, and the resulting evidence is available in a documented form.
3. **The wallet user authenticates for the issuance process.**
Where required by the scenario, the wallet user authenticates towards the issuer, or towards the relevant issuance environment, so that the issuance process can be associated with the correct natural person.
4. **The issuer performs identity binding.**
The issuer establishes and confirms the binding between the attestation subject, the relevant identity information, and the supporting assessment result or other underlying evidence, so that the micro-credential attestation can be issued to the correct natural person.
5. **The issuer confirms that the issuance conditions are satisfied.**
The issuer determines that the learning outcome claim is within scope, that the available evidence is sufficient, and that the applicable business, semantic, and governance conditions for issuance are fulfilled.
6. **The issuer creates the micro-credential attestation.**
The issuer prepares the micro-credential attestation in accordance with the applicable attestation model, including the relevant related attributes, identifiers, metadata, and, where applicable, validity or status information.
7. **The issuer issues the attestation to the wallet user.**
The Verified micro-credential attestation is issued to the wallet user and made available for transfer to the user's EUDI Wallet.
8. **The wallet user receives, reviews, accepts, and stores the attestation in the wallet.**
The wallet user receives the attestation in the EUDI Wallet, is given the opportunity to review its content, explicitly accepts its addition to the wallet under their control, and stores it for subsequent use.
9. **A relying party requests proof of the learning outcome.**
At a later stage, a relying party requests evidence of the relevant learning outcome or competence for a defined purpose, such as enrolment in a course at a university.
10. **The wallet holder authenticates to the wallet and authorises the presentation.**
The wallet holder authenticates to the EUDI Wallet and authorises the response to the relying party request, thereby ensuring that presentation of the micro-credential attestation takes place under the holder's control.
11. **The wallet user selects the relevant attestation.**
The wallet user identifies the appropriate micro-credential attestation in the wallet and prepares a response to the relying party's request.
12. **The wallet user presents the attestation.**
The wallet user presents the micro-credential attestation, or, where supported, the relevant subset of attested attributes, to the relying party through the EUDI Wallet.
13. **The relying party verifies the attestation.**
The relying party verifies the presented attestation in accordance with the applicable

verification rules, including checks relating to authenticity, integrity, validity status, issuer trust, and semantic interpretability.

14. The relying party evaluates the attested skill information for its purpose.

The relying party assesses the verified attestation against its own business, procedural, or operational requirements and determines whether the presented skill information is sufficient for the intended use.

15. The relying party determines the outcome of the transaction.

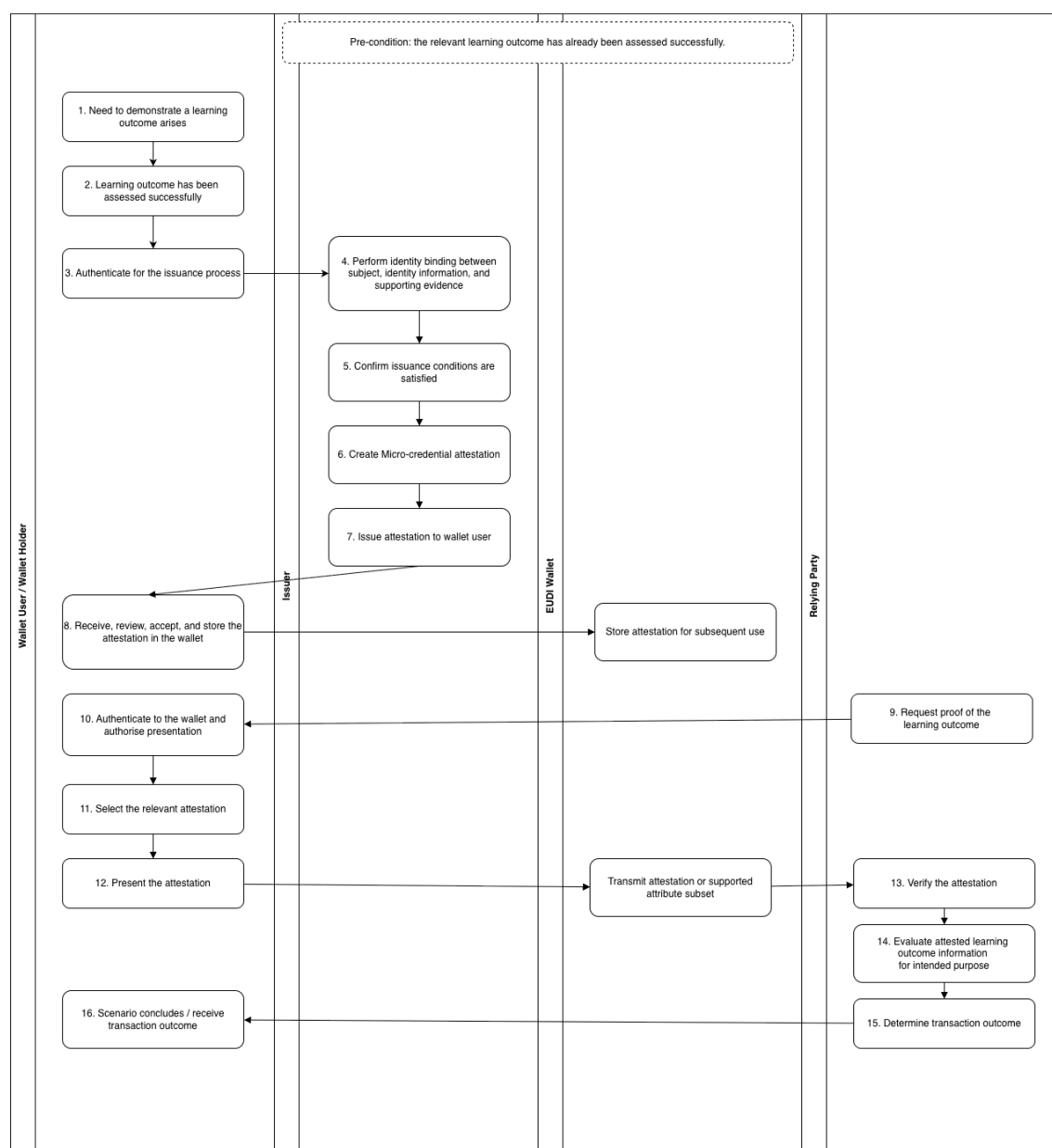
On the basis of the verification result and its own decision criteria, the relying party accepts the attestation, rejects it, or requests additional information or evidence.

16. The scenario concludes.

The interaction concludes with a business outcome, such as continuation of enrolment in a course or referral to an alternative process.

Per step in the main flow, a detailed description is made in the table below.

Micro-credential Attestation – Main Flow (with Identity Binding and Holder Authentication)



4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of EUDI Wallet	Linköping University	SE
	UAegan	GR
2. Authentic sources	Linköping University	SE
	UAegan	GR
3. Relying party	Linköping University	SE
	UAegan	GR
4. Intermediary	SUNET	SE

4.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	GRnet	Any	
	Gunet	Any	wwWallet
	Procivis	Any	Procivis One
	E-gov Moldavia	Any	Evo
	Sphereon	Any	Spherio n wallet
	SIROS	Any	SIROS ID
2. PID Provider			
3. Trusted list registrar	The general lists supplied by the WE BUILD project.		
4. QEAA provider	N/a in MVP		
5. Pub-EAA provider	N/a in MVP		
6. EAA provider	Authentic sources will provide their own credentials		
7. QES provider	N/a in BU5		

4.3 Target country combinations

	Issuing country						
Relying Party country		SE	GR				
	SE						
	GR						

4.4 Requirements

The main requirements for each of the roles involved in the Micro-credential scenario are set out in **Annex 1 – Requirements for scenario roles**.

The Annex provides the role-specific requirements relevant to the execution of the scenario, including requirements relating to issuance, assessment evidence, wallet functionality, presentation, verification, and relying-party acceptance.

To avoid duplication, those detailed requirements are not repeated in this section.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners), or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

In this scenario the only credential that will be provided by other scenarios is the PID credential.

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Personal Identification Data attestation used to support reliable identification of the wallet user and identity binding in the issuance flow, and where relevant to support presentation and verification in the relying-party flow.	WE BUILD PID providers	SE, GR	Must enable reliable linkage between the attestation subject and the Micro credential attestation.
Mock PID attestation	Test or pilot equivalent of the PID attestation, used in controlled environments where a production PID attestation is not available.			Must support the same scenario functions as the PID attestation for pilot or test purposes.

5.3 Created attestations in the scenario

The attestation that will be created in this scenario is the micro-credential.

Attestation name	Short description	For Countries	Applicable domain standards
Micro-credential	Micro-credential means the record of the learning outcomes that a learner has acquired following a small volume of learning.	SE, GR	

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Wallet User

Specific requirement
MUST be able to receive a Micro credential attestation in the wallet following completion of the issuance flow.
MUST be given the opportunity to review the attestation content before accepting its storage in the wallet.
MUST explicitly accept addition of the Micro credential attestation to the wallet before it is stored for subsequent use.
MUST be able to distinguish the Micro credential attestation from other attestations held in the wallet.
MUST be able to identify the issuer of the Micro credential attestation at the moment of review and presentation.
MUST be able to see the core skill claim or claims contained in the attestation in a human-understandable form.
SHOULD be able to view any stated assurance or quality level associated with the attestation, including where relevant Level 1 – Self-asserted, Level 2 – Third-party assessed, or Level 3 – Audited assessment.
SHOULD be able to view validity-related information associated with the attestation, such as issuance date, review date, expiry date, or current status, where applicable.
MUST authenticate and authorise presentation of the Micro credential attestation before disclosure to a relying party takes place.
MUST remain in control of whether the attestation is presented in response to a relying-party request.
SHOULD be able to present only the subset of attested information necessary for the relying party's purpose, where the attestation model and wallet support such selective disclosure.
SHOULD be able to present the Micro credential attestation together with other relevant attestations where the relying party requires combined evidence.

Issuer

Specific requirement
MUST issue the Micro credential attestation only where the relevant skill claim is supported by documented assessment evidence.
MUST perform identity binding between the attestation subject, the relevant identity information, and the supporting assessment evidence before issuing the attestation.
MUST issue the attestation only where the assessed skill is within the scope of the Micro credential use case as defined by the applicable governance and rulebook conditions.
MUST ensure that the attestation is issued to the correct natural person and made available to that person's wallet.
MUST include in the attestation a clear representation of the attested skill or competence.
MUST include sufficient metadata to support relying-party interpretation of the attested skill claim.
MUST include issuer-identifying information sufficient to support verification and relying-party

trust decisions.
SHOULD reference the attested skill using a recognised taxonomy or classification, such as ESCO/ISCED, where applicable.
SHOULD indicate the basis of assessment or evidential strength of the attestation where this is relevant for relying-party interpretation.
SHOULD indicate the applicable assurance or quality level of the attestation where such levels are defined by the Rulebook.
SHOULD include validity, review, renewal, or status information where the nature of the skill claim requires lifecycle management.

5.4 Authentic Source

Specific requirement
MUST provide authoritative identity-related or attribute-related source information where the Micro credential issuance flow relies on an authentic source for identity binding or source validation.
MUST ensure that any source information made available for the scenario can be linked to the correct natural person.
MUST provide source information only within the scope and mandate applicable to the scenario.
SHOULD provide source information in a form that can be interpreted consistently by the issuer for issuance purposes.
SHOULD support traceability of the source information used in the issuance process where this is required by governance or audit conditions.

5.5 PID Provider

Specific requirement
MUST provide a PID attestation, or equivalent pilot-capable PID artefact, that can support reliable linkage between the wallet user and the Micro credential attestation.
MUST support use of the PID attestation in the scenario for identity-related functions relevant to issuance and, where applicable, presentation.
SHOULD provide PID data in a form that supports consistent identity binding in the Micro credential issuance flow.

5.6 Trusted List Registrar

Specific requirement
MUST ensure that trust information relevant to acceptance of the Micro credential attestation can be made available in a way that supports relying-party verification of issuer trust status, where such trust registration is part of the scenario governance.
SHOULD support timely publication or update of trust information relevant to the scenario where issuer status, registration, or trust eligibility changes.
SHOULD ensure that trust information can be interpreted consistently by relying parties participating in the scenario.

5.7 Pub-EAA Provider

Specific requirement
MUST provide publicly verifiable Electronic Attestation of Attributes functionality where the scenario requires publication-oriented or publicly verifiable EAA support connected to the Micro

credential flow.

MUST ensure that public EAA information relevant to the scenario is made available in a form that supports relying-party verification and interpretation.

SHOULD ensure that the published EAA information remains consistent with the current attestation status and applicable lifecycle conditions.

EEA Provider

Specific requirement
MUST support issuance of the Micro credential attestation as an Electronic Attestation of Attributes in accordance with the attestation model applicable to the scenario.
MUST support inclusion of the metadata elements required for interpretation, verification, and lifecycle handling of the Micro credential attestation.
MUST support binding of the attestation to the correct attestation subject as established in the issuance process.
SHOULD support selective disclosure where such functionality is part of the Micro credential attestation model.
SHOULD support expression of assurance or quality levels where such levels are defined in the Rulebook.

5.8 EUDI Wallet Provider

Specific requirement
MUST support a same-device flow in which a relying-party request initiated on a website or equivalent interface can lead the user into the wallet for controlled presentation of the Micro credential attestation.
MUST support a same-device flow in which an issuer-side issuance journey initiated on a website or equivalent interface can lead the user into the wallet for controlled receipt and acceptance of the Micro credential attestation.
MUST present the attestation to the user for review before final acceptance and storage.
MUST require holder authentication and user authorisation before presentation of the Micro credential attestation to a relying party.
MUST support presentation of the attestation under holder control in response to a relying-party request.
SHOULD support selective disclosure of attested attributes where this is supported by the attestation model.
SHOULD display the core skill claim, issuer identity, and applicable validity or status information in a human-understandable form.
SHOULD display the applicable assurance or quality level in a human-understandable form where such a level is part of the attestation.
SHOULD enable the user to distinguish the Micro credential attestation from other wallet-held attestations.

5.9 Relying Party

Specific requirement
MUST request only the skill-related information necessary for the specific business, operational, educational, or administrative purpose.
MUST verify the authenticity and integrity of the presented Micro credential attestation before relying on it.
MUST verify the attestation status, including where applicable whether it is valid, expired,

superseded, suspended, or revoked.

MUST verify the identity of the issuer to the extent necessary to determine whether the issuer is acceptable for the relying party's purpose.

MUST distinguish between verification of the attestation and evaluation of whether the attested skill is sufficient for the relying party's purpose.

MUST evaluate the attested skill claim against defined acceptance criteria relevant to the intended use context.

MUST NOT treat successful cryptographic or technical verification alone as sufficient proof that the attested skill is acceptable for its purpose.

SHOULD be able to interpret any assurance or quality level associated with the attestation where such levels are used in the scenario.

SHOULD be able to interpret recognised taxonomy or classification references, such as ESCO references, where these are included in the attestation.

SHOULD support selective disclosure by accepting the minimum attested information necessary for the intended purpose, where supported by the attestation model.

SHOULD be able to evaluate the Micro credential attestation together with other supporting attestations where combined evidence is required.

SHOULD define fallback handling for cases in which the attestation cannot be accepted, including rejection, request for additional evidence, deferred decision, or referral to an alternative process.

WE BUILD consortium

Specification BU6 Scenario 1 – Full power access to OOTS

WP2 – BU6 Business access to OOTS

Date : 18-6-2026
Version : 1.0
Status : Final

Index

1	Introduction	3
1.1	<i>Objectives of this document.....</i>	3
1.2	<i>Scenario introduction.....</i>	3
2	Scenario specification.....	4
2.1	<i>Introduction</i>	4
2.2	<i>Scenario pre-conditions</i>	4
2.3	<i>Scenario main flow</i>	5
2.4	<i>Scenario additional flows.....</i>	6
2.5	<i>Challenges and barriers</i>	6
2.6	<i>Working Assumptions</i>	7
3	Detailed scenario flow.....	8
4	Roles and participants	13
4.1	<i>Scenario roles and participants.....</i>	13
4.2	<i>Additional roles and partners</i>	14
4.3	<i>Target country combinations.....</i>	14
4.4	<i>Requirements.....</i>	14
5	Attestations	15
5.1	<i>Introduction</i>	15
5.2	<i>Attestations to be provided by other UCs/WGs/scenarios.....</i>	15
5.3	<i>Created attestations in the scenario</i>	16
	Annex 1 – Requirements for scenario roles.....	18
	Annex 2 – <name>.....	19

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 1, as part of use case BU6 in work package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

Out of scope of this scenario are: the use of a fine grained power to represent the company and the use of the European business wallet (EBW).

1.2 Scenario introduction

In BU6 scenario 1 the user will, on behalf of a company, apply for a service in the business domain and the user will use the OOTS to provide information to the relying party. During this process the user will use the EUDI-wallet to authenticate and prove full powers to represent the company. The user will do this not only at the relying party member state but also at the evidence providing member state.

The scenario is based on the following documentation:

- WE BUILD WP4 Conformance specifications and Architecture Decision Record (ADR's)
- The BU6 stock taking document final version (1.0)
- OOTS TDD version 1.2.3
- Relevant WP4 documentation
- Relevant taking stock 1st generation documentation
- Relevant SDG-OOTS documentation

2 Scenario specification

2.1 Introduction

The overall goal of the use-case is to explore integration of the EUDI Wallet and the Single Digital Gateway Once Only Technical System (SDG OOTS). These are two different channels for the user to provide personal and company data to relying parties. With BU6 we explore the possibilities of the user to mix these channels in a way most convenient to them.

Scenario 1 of BU6 has the goal to evaluate the use of the EUDI Wallet by a natural person with full powers to represent a company, as a means to authenticate at the relying party and to reauthenticate at the OOTS preview space, as an alternative for a national or eIDAS notified eID.

2.2 Scenario pre-conditions and dependencies

The main prerequisites and related responsibilities of BU6 are:

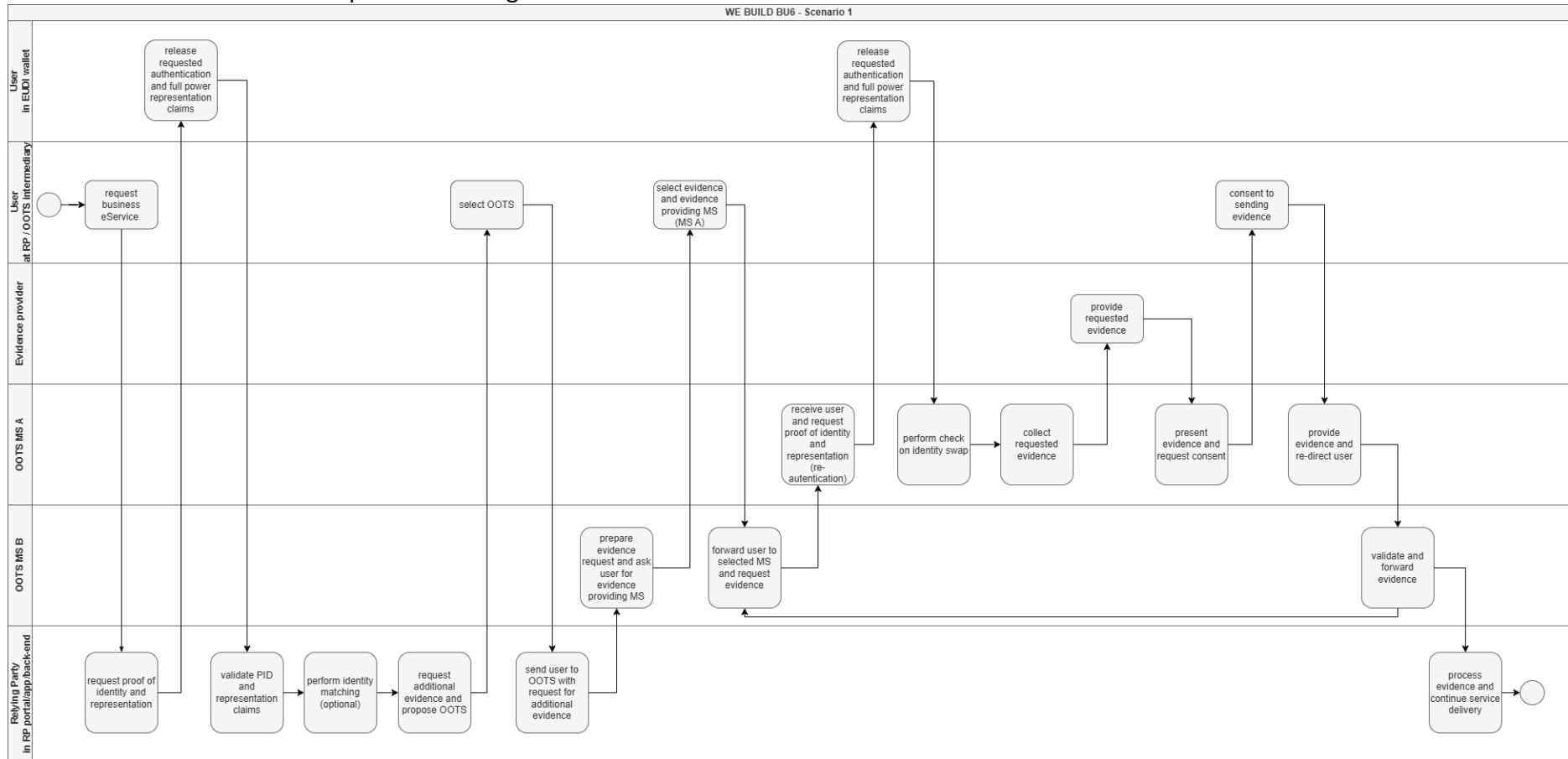
1. Availability of the PoR rulebook: BU4/WP4 Semantics group.
2. Availability of the PID rulebook: WP4 PID group.
3. Availability of EUDI Wallets: WP4 Wallet group.
4. PID attestations issued to the EUDI-wallets: WP4 PID group.
5. Clear technical specifications (WE BUILD Conformance Specifications - WBCS) and change management on these specifications: WP4 Architecture group.
6. Clear WB Trust framework, integrated in WBCS.
7. Participants have taken care of a working, connected and tested OOTS implementation: BU6 participants.
8. Availability of the, by BU6 participants agreed upon, OOTS evidence type to be exchanged between piloting member states; the company registration evidence type: BU6 participants.

The main external prerequisites of BU6, falling entirely outside the scope and effort of the BU6 consortium, are:

1. Availability of OOTS Commons services (acceptance and production environment): European Commission.
2. Updated OOTS technical specifications to support the use of PID attributes (nice to have, work-around available): European Commission.
3. Availability of the OOTS procedural requirement 'Proof of existence of a legal person (basic information)': European Commission.

2.3 Scenario main flow

The detailed scenario flow is depicted in the figure below.



2.4 Scenario additional flows

The main focus of the scenario is on the happy flow. One exception will be piloted: the failed identity swap check at the OOTS intermediary platform resulting in an error message and the ending of the process.

Flow	Short description
- Happy flow	The main flow where the user can apply for the service on behalf of the company and can provide evidence via OOTS to the relying party.
Exceptions	
- E01 – Identity swap	After re-authentication an identity swap is noticed by the OOTS intermediary platform at MS B, meaning a person re-authenticated other than the person that authenticated at the relying party. This results in an error and the termination of the process.

2.5 Challenges and barriers

The development and piloting of the proposed solution involve a range of technical, legal/regulatory, and operational challenges. These stem from the evolving nature of the European Digital Identity ecosystem, the ongoing processes and variations of the OOTS implementation at national level, dependencies across multiple stakeholders, and the current maturity of supporting frameworks and infrastructures.

2.5.1 Technical Challenges

A key technical challenge relates to the continuous evolution of the Architecture and Reference Frameworks (ARFs). As these specifications are updated during the project lifecycle, pilot implementations must be regularly adapted to maintain compliance, increasing development complexity and effort. Closely linked to this is the emergence of new or refined technical requirements during the specification phase, which may not be fully aligned with the initial system architecture.

Interoperability also presents a significant barrier. Differences in credential formats and protocols between EUDI Wallet implementations and relying parties may hinder seamless cross-border interactions. Similarly, inconsistencies in the implementation versions of the Once-Only Technical System (OOTS) across Member States can lead to integration failures or unreliable data exchanges.

2.5.2 Legal and Regulatory Challenges

The regulatory landscape is still evolving, creating uncertainty for implementation. Key implementing acts under the eIDAS Regulation—particularly those concerning Electronic Attestations of Attributes and the EU Digital Identity Wallet—are still under development or expected to be finalized during the project timeline. For example, technical specifications for the EU Company Certificate and the Digital Power of Attorney are anticipated by mid-2026, creating a temporary regulatory gap.

At the national level, several Member States currently lack specific legal frameworks applicable to this use case. In countries such as Greece and Portugal, no dedicated legislation exists yet, while in others, such as Poland and Slovenia, relevant laws are still under preparation. This lack of harmonization may delay implementation and complicate cross-border interoperability.

Additional legal complexity arises from fragmented data sources and registries. For instance, in some Member States there is no unified register for Powers of Representation, which complicates the verification and issuance of attestations. Furthermore, the absence of widely available electronic identification means for legal persons and their representatives remains a barrier to full digitalization of the process.

2.5.3 Operational Challenges

Operationally, the pilot depends on coordination among a large number of organizations across different domains and countries. This creates a dependency risk since failure or delay by a single participant may impact the overall success of the pilot scenario.

Effective communication and coordination mechanisms are therefore critical but challenging to maintain, especially given the need to align with multiple work packages, architecture groups, and external stakeholders. Managing changes in specifications, ensuring all participants remain aligned, and resolving misunderstandings in a timely manner require structured governance and continuous engagement.

Finally, the need for continuous interaction with technical governance bodies—such as Architecture and Test Infrastructure groups—adds complexity but is essential to ensure that the developed solution remains compliant, interoperable, and fit for purpose.

2.6 Working Assumptions

No significant working assumptions are required. Nevertheless, in practical terms, the learning outcomes can be:

- 1) How the EUDIW can be used to initiate or support OOTS transactions by allowing users to authenticate to public portals,
- 2) How to authorize the retrieval of evidence through OOTS.

These create a coherent flow where OOTS handles trusted data exchange in the background, while the EUDIW acts as the secure, user-controlled interface for interaction, transparency and reuse. The combined use of EUDIW and OOTS strengthens trust, interoperability and user experience in EU cross-border public services, reduces administrative burden, and supports the delivery of fully digital, once-only public procedures under the Single Digital Gateway and eIDAS 2.0 frameworks.

All the OOTS services, requirements, evidence types, evidences, and data providers required should be registered to the acceptance dashboard of the OOTS common services.

3 Detailed scenario flow

Per step in the main flow as depicted in section 2.3, a detailed description is made in the table below.

In the Table, a user from Member State A needs to complete a business procedure in Member State B on behalf of a company. In doing so, the user authenticates using the EUDI Wallet and provides the required evidence through the Once-Only Technical System (OOTS), enabling the relying party in Member State B to retrieve and verify the necessary information from the relevant authorities.

Main flow step	Actor	Description and reference	Variations and exceptions
Request business eService	User	User navigates to RP-portal in another member state. User starts applying for a public SDG cross-border business eService and clicks on 'Logon on behalf of company' or similar user action to start the process. Reference: - RP specific	
Request proof of identity and representation	RP	RP performs user authentication. It creates a request for unique PID-set and full power 'Power of Representation' (PoR) attestation and sends the request to EUDI-wallet. RP can use a wallet handling intermediary to perform authentication. Reference: - WBCS and ADR's - WB Trust framework - PoR rulebook - PID rulebook	
Release requested authentication and full power representation claims	User	User opens EUDI-wallet, checks request, consents to sending claims (unique PID set and PoR attestation) to RP and sends response to RP. Reference: - WBCS and ADR's - WB Trust framework - UX/UI guidelines	

Validate PID and representation claims	RP	RP receives and validates the response. Reference: - WBCS and ADR's - WB Trust framework	
Perform identity matching (optional)	RP	RP performs identity matching on the natural person (optional, RP specific). The natural person is registered in the relying party systems if not found (optional, RP specific). Reference: member state specific design.	
		RP performs identity matching on the legal person (optional, RP specific). The legal person is registered in the relying party system if not found (optional, RP specific). Reference: member state specific design.	
Request additional evidence and propose OOTS	RP	After granting access the RP informs the user that additional evidence (on the registration of the company) is needed and that the user can (amongst other options) select the OOTS to provide this evidence. Reference: member state specific design.	
Select OOTS	User	On the RP portal the user selects OOTS to provide additional information for one specific evidence that is required. Reference: member state specific design.	
Send user to OOTS with request for additional evidence	RP	RP redirects user to the OOTS intermediary platform of MS B. If the RP implemented its own OOTS functionality this step is skipped. Reference: member state specific design.	

Prepare evidence request and ask user for evidence providing MS	OOTS IP MS B	The OOTS intermediary platform (or RP OOTS functionality) prepares the evidence request based on the RP requirement and asks the user to select the evidence type and member state. Note that specific OOTS functionality (for instance the communication with the common services) is not detailed out in the figure. Reference: OOTS TDD and member state specific design.	
Select evidence providing MS (MS A)	User	The user selects the evidence type and the country (MS A) that will provide the evidence. Reference: OOTS TDD and member state specific design.	
Forward user to selected MS and request evidence	OOTS IP MS B	The OOTS intermediary platform (or RP OOTS functionality) of MS B sends the request to MS A and forwards the user to the OOTS intermediary platform of MS A. Reference: OOTS TDD.	
Receive user and request proof of identity and representation (re-authentication)	OOTS IP MS A	The OOTS intermediary platform of MS A receives the user and the evidence request. The OOTS intermediary platform (or intermediary) creates request for unique PID-set and full power 'Power of Representation' (PoR) attestation and sends request to EUDI-wallet. OOTS IP can use a wallet handling intermediary for the authentication. If needed additional attestations can be requested, this is optional and member state specific (e.g. specific member state identifier). Reference: - OOTS TDD - WBCS and ADR's	
Release requested authentication and full power representation claims	User	User opens EUDI-wallet and checks request. Reference: - WBCS and ADR's	

		- WB Trust framework	
		User consents to sending claims (unique PID set and complete PoR attestation) to OOTS IP / intermediary and sends response to OOTS IP / intermediary. Reference: - WBCS - UX/UI guidelines	
Perform check on identity swap	OOTS IP MS A	After re-authentication the OOTS IP compares the natural and legal person data with the data received from MS B in the OOTS request. Reference: OOTS TDD.	E01 - Failed identity swap check
Collect requested evidence	OOTS IP MS A	The OOTS intermediary platform of MS A requests the evidence from the evidence provider. Reference: OOTS TDD.	
Provide requested evidence	Evidence provider	The evidence provider receives the request for evidence and uses the information in the request to collect data from the authentic source and sends it to the OOTS intermediary platform. Reference: OOTS TDD and member state specific design.	
Present evidence and request consent	OOTS IP MS A	The OOTS IP MS A presents the collected data in the preview space and requests consent from the user to send the data to the MS B. Reference: OOTS TDD.	
Consent to sending evidence	User	The user checks the presented data and consents to sending the evidence to the RP in the other MS. Reference: OOTS TDD.	

Provide evidence and re-direct user	OOTS IP MS A	The OOTS IP MS A sends the evidence to the OOTS IP of MS B and redirects user to the RP Portal of MS B. Reference: OOTS TDD.	
Validate and forward evidence	OOTS IP MS B	The OOTS IP of MS B receives and forwards the response after technical validation to the RP. If the RP implemented its own OOTS functionality this step is skipped, the RP will have received the evidence directly in the previous step. If more evidence is needed and selected by the user, the OOTS-process can be repeated. This is optional and member state specific. Reference: OOTS TDD and member state specific design.	
Process evidence and continue service delivery	RP	The required additional information and the user is received and service delivery continues. Reference: OOTS TDD and member state specific design.	

4 Roles and participants

4.1 Scenario roles and participants

MEMBER STATE OF RELYING PARTY (REQUESTING MS / MS B)		
Primary role	UC partner Name	MS
1. Relying party	GRNET/MoDG	EL
	MRIT/PIT	PL
	GOV.PT/Auth.Gov	PT
	MDT	SI
2. Intermediary for wallet authentication on behalf of Relying party (optional)	No wallet services intermediary will be used	EL
	PIT	PL
	No wallet services intermediary will be used	PT
	SI-PASS (MDP)	SI
3. OOTS Intermediary Platform connected to Relying Party (optional, RP can implement this functionality)	GRNET/MoDG	EL
	MRIT/PIT	PL
	ARTE	PT
	MDT	SI

MEMBER STATE OF AUTHENTIC SOURCE (PROVIDING MS / MS A)		
Primary role	UC partner Name	MS
4. User of EUDI Wallet		
5. Evidence provider connected to OOTS	MoDG	EL
	MRIT	PL
	IRN/RNPC	PT
	MDT	SI
	KVK	NL
6. Authentic source PoR (Implementation and testing of these components remains under the scope of BU6)	GRNET/MoDG	EL
	MRIT	PL
	ARTE	PT
	MDT	SI
	KVK	NL
7. OOTS Intermediary Platform connected to Evidence provider	No OOTS intermediary platform will be used	EL
	MRIT	PL
	ARTE	PT
	MDT	SI
	RINIS	NL
8. Intermediary for wallet authentication on behalf of OOTS re-authentication (optional)	No wallet services intermediary will be used	EL
	PIT	PL
	No wallet services intermediary will be used	PT
	No wallet services intermediary will be used	SI
	No wallet services intermediary will be used	NL

4.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	GRNET/MoDG	EL	
	Ministry of Digital Affairs (MC)	PL	
	ARTE	PT	
	MDT	SI	
	KVK	NL	
2. PID Provider	GRNET/MoDG	EL	
	MC	PL	
	ARTE	PT	
	MDT	SI	
	KVK	NL	
3. QEAA/Pub-EAA provider (PoR)	GRNET/MoDG	EL	
		PL	
	ARTE	PT	
	MDT	SI	
	KVK	NL	

4.3 Target country combinations

	Issuing MS					
		EL	PL	PT	SI	NL
Relying Party MS	EL		Y	Y	Y	Y
	PL	Y		Y	Y	Y
	PT	Y	Y		Y	Y
	SI	Y	Y	Y		Y

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex.

5 Attestations

5.1 Introduction

BU6 Scenario 1 will use the PID and PoR (Power of Representation) attestations. They will be used to authenticate and identify the natural person and to ascertain the full powers of this natural person to act on behalf of a certain company / legal person.

In addition to the EUDI-wallet attestations an OOTS evidence type will be used to exchange information regarding the company / legal person between the piloting member states.

Power of Representation attestation

A power of representation attestation is needed in BU6-scenario 1. With this attestation the natural person can prove the full power to act on behalf of the company. Note that fine grained powers validation is in scope of scenario 2.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	The PID is used to authenticate and identify the natural person acting on behalf of a company.	WP4 – PID Group (design and issuance is part of WP4)	Issuing: EL, PL, PT, SI, NL Requesting: EL, PL, PT, SI, NL	The PID contains: - The mandatory attributes to identify the natural person. - The optional attributes that are needed, in addition to the mandatory attributes, to uniquely identify the natural person. This can vary per member state. No other functionalities are piloted other than plain, happy flow authentication with standard validation (for instance Revocation or overasking are not piloted).
PoR	To deliver a service in the business domain, the relying party needs to be able to validate in real-time that the user is entitled to act on behalf of a legal person for this service, to ascertain the legal basis to deliver this service. See also Potential Rulebook Power of Representation v1.2 High level requirements:	BU4 (design is to be provided by BU4, issuance is part of BU6)	Issuing: EL, PL, PT, SI, NL Requesting: EL, PL, PT, SI, NL	The PoR contains: - Identifier of the legal person on which the holder of the wallet has representational powers. - Current legal name of the legal person identified with the legal person identifier as declared in the first attribute.

	1. The relying party must not need to interpret the PoR attestation with additional algorithms or business rules, especially if these algorithms or business rules are member state specific. Receiving and validating the PoR attestation should be sufficient to grant access to the user to act on behalf of the company. 2. The attestation can provide a full power of representation which indicates that the user can act on behalf of a specific company for all SDG services in other member states. 3. The attestation can provide a fine-grained power of representation which indicates that the user can act on behalf of the company for a specific SDG service in other member states. 4. The attestation provides the validity period of the power of representation so the relying party can validate if the power of representation is active.			- Indication whether natural person has full powers to represent the company. - Date from which the power to represent the company is effective. The date is included in the validity period, so on this date the powers are valid. - Date until which the power to represent the company is effective. The date is included in the validity period, so on this date the powers are valid. Regarding the attribute eService the following integrity rules hold: - If the value of the data element 'full_powers' is 'true', then the data element 'eService' SHALL be empty. - If the value of the data element 'full_powers' is 'false', then the data element 'eService' SHALL not be empty. Regarding the attribute effective_until_date the following integrity rule holds: - If provided, the data element 'effective_until_date' SHALL be greater than the 'effective_from_date' data element.
--	---	--	--	---

5.3 Created attestations in the scenario

No attestations will be created in BU6 scenario 1.

For the OOTS evidence type used in the scenario the evidence type needs to be accepted by the OOTS evidence mapping group and needs to be registered in the OOTS common services (see [OOTS evidence explorer](#)). The registration needed is as follows:

- An OOTS **Procedural Requirement** is registered in the Common Services: the procedural requirement 'Proof of existence of a legal person (basis information)' is registered in Acceptance and Production and will be used. The description of this Procedural

Requirement is: “Request for evidence regarding the existence and legal capacity of a legal person with only the basic information. Indicative (non-exhaustive) information that the supporting evidence may contain: (1) legal name of evidence subject (legal person) (2) confirmation of existence of the evidence subject (legal person) (3) confirmation of legal capacity of the evidence subject (legal person)”.

- Participating Relying Parties have registered an OOTS **Procedure** that is linked to the Procedural Requirement. Example: SI have registered the Procedure ‘Notification of temporary pursuit of craft activities’.
- Evidence providers need to create an **Evidence** and to link this evidence type to the procedural requirement. Example: the Slovenian Business Register has registered the evidence ‘Proof of registration in the country of establishment’ which is linked to the Procedural Requirement.

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUDI Wallet	a. All BU6 partners MUST take care for the users
	b.
	c.
2. Authentic sources	a. See previous table for PoR (EL, PL, PT, SI, NL). COULD use synthetic data (in collaboration with the authoritative source)
	b.
	c.
3. Relying party	a. MUST be able to receive and evaluate PID and PoR attestations. See previous table for relying parties (EL, PL, PT, SI, NL)
	b.
	c.
4. Intermediary for wallets	a. Optional role
5. OOTS Intermediary	b. Optional role
6. EUDI Wallet provider	a. Wallet MUST accept PIDs from EL, PL, PT, SI, NL
	b. Wallet MUST accept PoR attestation from EL, PL, PT, SI, NL
	c.
7. PID Provider	a. EL, PL, PT, SI, NL PIDs MUST be available
	b.
	c.
8. Trusted list registrar	a. Required - WP4 MUST take care
	b.
	c.
9. QEAA provider	a. MUST be able to issue PoR attestations (Member State Specific)
	b.
	c.
10. Pub-EAA provider	a. MUST be able to issue PoR attestations (Member State Specific)
	b.
	c.
11. EAA provider	a. MUST be able to issue PoR attestations (Member State Specific)
	b.
	c.
12. QES provider	N/A

WE BUILD consortium

eCMR/eFTI compliant cross border transport by connecting electronic cargo waybill datasets with Business Wallets

WP2 – SC1 – Authentication and access for transport

Date : 16/07/2026
Version : V1.0 16/07/2026
Status : Final

Index

1 Introduction	3
1.1 Objectives of this document	3
1.2 Scenario introduction	3
2 Scenario specification	4
2.1 Introduction	4
2.1.1 SC1.3 (MVP) – eCMR creation via the Business Wallet	5
2.1.2 SC1.3bis (MVP+) – control via the eFTI network or not	5
2.2 Scenario pre-conditions	6
2.3 Scenario main flow	7
2.4 Scenario alternate flow	7
2.5 Challenges and barriers	7
2.6 Working Assumptions	8
3 Detailed scenario flow	8
3.1 SC1.3 MVP – eCMR lifecycle	8
3.2 SC1.3bis MVP+ – control with or without the eFTI network	12
4 Roles and participants	14
4.1 Scenario roles and participants	14
4.2 Additional roles and partners	15
4.3 Target country combinations	15
4.4 Requirements	16
5 Attestations	17
5.1 Introduction	17
5.2 Attestations to be provided by other UCs/WGs/scenarios	17
5.3 Created attestations in the scenario	17
Annex 1 – Requirements for scenario roles	19

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario SC1.3 “eCMR/eFTI compliant cross border transport by connecting electronic cargo waybill datasets with Business Wallets”, as part of use case SC1 “Authentication & access for transport” in work package 2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, the attestations to be used and the partners that are involved in creating solutions and piloting.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

1.2 Scenario introduction

eCMR and eFTI – what they are. An eCMR is the electronic equivalent of the international road consignment note (CMR): the document that accompanies a road shipment and records the consignor, carrier, consignee, goods and the handover events. eFTI (electronic Freight Transport Information) is the EU framework – Regulation (EU) 2020/1056 and Implementing Regulation (EU) 2024/1942 – that lets businesses make regulatory freight data available to competent authorities in electronic form. In this scenario the two come together for enforcement: the eCMR is the consignment dataset, and eFTI is the channel through which a control authority can access that dataset during a roadside check.

This scenario covers the handover and the control of a cargo while it is in transit on the road. Its purpose is to demonstrate:

- [SC1.3 – MVP] How the handover of the goods between parties can be made easier, avoiding a dedicated onboarding for each party. The Business Wallet facilitates the platform connection and reduces the onboarding burden for all parties; it identifies the parties with the legal entity’s identity, which serves as a e-seal for the exchanges and removes the need for individual personal signatures.
- [SC1.3bis – MVP+] How a competent authority (control officer) can verify, at the roadside or at a control point, the freight transport information of the consignment, by combining two layers: the Business Wallet layer (the carrier’s enterprise identity – EBWOID – and an eCMR attestation carried in the driver’s Business Wallet, available as a mobile app client) and the eFTI network layer (the authoritative consignment dataset held on an eFTI Platform and queried through the national eFTI Gate by means of the Unique Identification Link, UIL).

SC1.3 is the natural continuation of SC1.2 Where SC1.2 addresses the terminal gate, SC1.3 covers the handover events and the in-transit enforcement check further along the road. The two scenarios are designed to be pilotable independently of one another: SC1.3 does not require SC1.2 to have been executed for the same consignment. Its own pre-conditions (2.2) only require that a consignment dataset has been registered and a UIL issued, whatever the origin of that registration.

The novelty of SC1.3bis is to bind the two layers through the UIL carried in the eCMR attestation, so that the credential the driver presents and the data the authority retrieves over the eFTI network refers to the same consignment.

Scope of the scenario:

- In scope (MVP and MVP+): road transport; EU cross-border; control performed by a competent authority; presentation of the eCMR attestation and EBWOID from the Business Wallet; the eCMR attestation; the advanced electronic seal; and retrieval of the authoritative consignment data via the eFTI network.
- Out of scope: the wider enforcement checks performed at the same time (vehicle weight, ADR/dangerous goods, driving and rest times, transport permit, driver licence); redesign or replacement of national eFTI Gates and eFTI Platforms; exchanges between eFTI Platforms; the qualified electronic seal; non-EU jurisdictions; rail and inland waterways.

The scenario assumes the availability of compliant Business Wallets and of an eFTI Platform / eFTI Gate from participating Member States; it does not develop the wallet itself, although developments needed for piloting are addressed in WP4.

2 Scenario specification

2.1 Introduction

SC1.3 is delivered in two parts.

In the MVP (SC1.3) the eCMR is created, signed and controlled through the Business Wallet and a single eCMR/eFTI platform. The Business Wallet's role is mainly to attest the parties – using the legal-entity identity from a business register or another recognised register, which the wallet then uses – and to provide authentication and digital signatures. It does not hold business logic or display business data, which remain the responsibility of the eCMR/eFTI platform.

Comment: The current eCMR and eFTI data models do not include native elements for digital signatures or electronic seals (e-seals), and the eFTI Regulation itself does not articulate clear provisions regarding the evidentiary validity of such signatures. This is a notable gap, given that the eCMR is fundamentally a business document — a contract of carriage establishing rights and obligations between consignor and consignee — for which a clear framework for signature validity and authenticity would normally be expected. It should be emphasized, however, that the aim of this project is not to amend or propose changes to the underlying legal framework. Rather, the objective is to explore, within the existing regulatory boundaries, practical approaches for establishing the authenticity of business document data and the validity of the actions taken by the parties involved.

In the MVP+ (SC1.3bis) The first variation is deliberately simplified: control queries do not travel over the eFTI network – the consignment data is shown directly from the platform (the request and the answer are exchanged over the public internet based on a QR code).

A second variation is that the control is performed through the eFTI network rather than directly from the driver's device: the eCMR data is linked to the eFTI network, the UIL is registered in the eFTI Gate, and the authority handles the control through an Authority Access Point (AAP), the eFTI Gate and a (pre-)certified eCMR/eFTI platform. This part depends on a working eFTI Gate-to-Platform query.

2.1.1 SC1.3 (MVP) – eCMR creation via the Business Wallet

An eCMR and a paper CMR are legally and procedurally equivalent; however, processing the data digitally also requires digital signing – which, in certain cases, may take the form of an electronic seal (a digital stamp of the legal entity) rather than a personal signature. The business workflow is as follows:

- Transport order preparation: the shipper (using a transport management or ERP system) creates the eCMR electronically and enters the mandatory transport information. A unique eCMR/eFTI identifier (UIL) is generated and the document is made available to the relevant parties.
- Driver arrival at pickup location: the driver identifies the shipment. The shipper and the driver verify that the goods correspond to the transport order. Any visible issues (damaged packaging, missing pallets, etc.) can be recorded as reservations.
- Pickup confirmation: once loading is complete, the shipper signs the eCMR electronically and the driver/carrier signs electronically. The eCMR becomes the official transport document.
- Arrival at delivery location: the consignee verifies the shipment; goods are checked against the eCMR information; quantities and condition are inspected.
- Delivery confirmation: after unloading, the consignee signs electronically and the driver signs as well. Delivery date, time and location are recorded, and any delivery remarks are attached.
- eCMR closure: after successful delivery the eCMR is locked against unauthorised changes; a final, legally valid version is generated and made accessible to the shipper, carrier, consignee and other authorised parties. The document is then archived and available for invoicing, claims management, customs audits and regulatory inspections. For cabotage inspection, the UIL remains open to authorities for 14 days [to be verified against the applicable cabotage rules].

In the scenario the business flow is simplified (happy path):

- Platform-managed: the entire eCMR lifecycle and its attestations are managed centrally by a single platform; data sharing between platforms is out of the happy path.
- No wallet-to-wallet exchange: the eCMR is never transferred directly between user wallets – all interactions go through the platform to keep a single source of truth.
- Most complex logistics cases are not addressed: subcarriers and multiple platforms will be handled by the platforms.
- Logistics edge cases are not piloted in the happy path: partial acceptance, reservations, quantity discrepancies, refusal, damaged goods, trailer changes, delays, etc.

2.1.2 SC1.3bis (MVP+) – control via the eFTI network or not

During the journey (SC1.3), the eCMR accompanies the shipment digitally. Authorities, customs officers or logistics partners can access the data (stored on the eCMR platform) when authorised, and events can be added. In a control event the request and the answer are exchanged over the public internet on the basis of the QR code: the control officer asks the driver to present the transport document; the driver opens the Business Wallet on the mobile device (phone or tablet) and, after authorising, shows the human-readable copy of the eCMR data (PDF).

A second variation is that the control is handled through the eFTI network and no longer directly from the driver's device. The eCMR data is linked to the eFTI network, the UIL is registered in the eFTI Gate, and the authority performs the control with an Authority Access Point (AAP), the eFTI Gate and a (pre-)certified eCMR/eFTI platform.

A driver, employee of carrier company A (country A), is transporting a consignment and is stopped for a control by a competent authority in country B. The driver uses a mobile device where the application, after driver's authorisation will present the document from Business Wallet (or copy, so a proximity flow with offline capability (the control may take place where connectivity is poor). The consignment dataset (eCMR) has been registered on an eFTI Platform and is referenced by a UIL.

The control officer needs to (a) establish who is carrying the goods (carrier and driver) and (b) obtain the authoritative consignment data. Two complementary verification paths are used:

- Wallet path: the driver presents the EBWOID (carrier identity) and the eCMR attestation from the Business Wallet.
- eFTI network path: the authority resolves the UIL through its national eFTI Gate and retrieves the authoritative consignment data from the eFTI Platform (Gate-to-Gate).

The following attestations will be processed:

- EBWOID of company A (carrier identity held in the Business Wallet);
- eCMR attestation including the UIL – the eCMR attestation and the eFTI QR code/UIL are issued and presented as a single credential and a single process; the eFTI-network part (UIL resolution over the Gate) is optional and is exercised only in MVP+.

Legal note. Under Implementing Regulation (EU) 2024/1942 the UIL is intended for competent-authority access to eFTI data. In SC1.3bis the relying party IS a competent authority, so the UIL-based query is the canonical, lawful use of the eFTI network – a key contrast with SC1.1 and SC1.2, where the relying party (a Port Community System) is a private body.

Device requirements (driver).

The driver uses the mobile application of Business Wallet on a smartphone or tablet. For the in-transit control the application present the human-readable eCMR (generated by eFTI Platform) to authorise the credential. The offline proximity presentation (used in MVP+) additionally requires suitable hardware [to be specified by WP4 – e.g. NFC support, a secure element/keystore, a camera for QR, and sufficient storage], so that the driver can use the mobile wallet reliably at the roadside even where connectivity is poor.

2.2 Scenario pre-conditions

- All actors hold a Business Wallet with an EBWOID issued by a competent authority that is on a Trusted List; the EBWOID carries the technical identity (public key) used to sign the carrier's attestations.
- The driver and all actors hold the Business Wallet as a mobile app client (issued and managed by the employer) containing the legal-entity identifier (EBWOID).
- The consignment dataset has been registered on an eCMR/eFTI Platform and a UIL has been issued for it.

- [SC1.3bis] The eFTI Platform is connected to a national eFTI Gate; the competent authority can reach the Gate (directly or via an intermediary) to perform a Gate-to-Business (G2B) query.
- [SC1.3bis] The competent authority is recognised to perform eFTI queries (officer authorization).
- The wallet trust infrastructure (Trusted List) and, in MVP+, the eFTI Gate / Platform are reachable for online verification; an offline fallback is defined for the proximity check.

2.3 Scenario main flow

In the MVP the eCMR is created, signed and exchanged via the platform and the Business Wallet. the full lifecycle steps are detailed in Figure 1 (section 3.1).

In the MVP+, a roadside control is answered directly from the platform based on the QR code; A second way is that the driver presents the EBWOID and the eCMR attestation, and the authority retrieves and cross-checks the authoritative consignment data through the eFTI network; that flow is shown in Figure 2 (section 3.2).

2.4 Scenario alternate flow

Intended variations to be piloted and investigated in testing / piloting.

Flow	Short description
Offline / wallet-only control	No connectivity at the control point. The authority relies on the eCMR attestation alone (proximity flow); the eFTI network query is deferred or skipped.
Handover / delivery acceptance	At delivery a discrepancy is recorded (e.g. 19 of 20 packages). To keep the happy path simple, the linking of a new eCMR attestation to the previous one is treated as optional / out of scope for the pilot.
Sole trader	The driver is the legal representative of the carrier and uses the carrier's own Business Wallet.
Cross-border Gate-to-Gate	The control authority in country B queries an eFTI Platform / Gate registered in country A; the request is routed Gate-to-Gate over the eFTI network.

2.5 Challenges and barriers

ID	Level	Challenge
1	High	Binding the wallet credential to the authoritative eFTI record. Ensuring that the eCMR attestation presented and the data retrieved via the UIL refer to the same consignment and detecting any tampering or mismatch (integrity matching on the envelope fields issuer_id / ecmr_attestation_id).
2	High	Roadside connectivity – proximity and online. The control may need both an offline proximity presentation and an online eFTI query. A robust fallback and clear outcome semantics (what is decided when only one path is available) are required.

ID	Level	Challenge
3	Medium	eCMR attestation versioning / linking. Rulebook v1.0 does not yet resolve linked or updated attestations needed for the handover flow; some formats (e.g. SD-JWT) do not natively support linked data.
4	Medium	Revocation freshness. The status of the EBWOID must be checked close to real time at the roadside; short-lived credentials or status lists must balance security and usability.
5	Medium	Cross-border Gate-to-Gate trust. The querying authority's Gate must be trusted by the platform's Gate; non-matching national identifiers complicate carrier mapping (as already noted for non-Dutch organisations in SC1.1).
6	High	Business Wallet functional capability for the roadside proximity flow. It must be confirmed with WP4 / the wallet provider whether the Business Wallet client can (a) operate the offline/proximity presentation reliably, (b) render the human-readable eCMR as a PDF for the officer, and (c) meet the device requirements listed in 2.1.2 (NFC, secure element, camera). Until confirmed, this is an open dependency for MVP+ piloting.

2.6 Working Assumptions

- A Business Wallet available as a mobile app client, as defined in the SC1.2 pre-conditions, is available. See Challenges and barriers, item 6 (2.5) for the specific capabilities still to be confirmed.
- Business registers can issue an EBWOID, or a QTSP will do it where business registers are not available for the expected countries.
- An eFTI Platform holding the consignment data and a reachable national eFTI Gate are available in the pilot, with a UIL issued per consignment.
- The eCMR attestation follows rulebook v1.0 (UN/CEFACT eCMR D24A) with the added wallet envelope object.
- Only test data and a pre-production environment will be used.

3 Detailed scenario flow

As a pre-requisite, the driver has a mobile device (provided or not by the enterprise) on which the Business Wallet has been set up and is accessible to present attestations only by that same driver. The consignment data has been registered on an eCMR/eFTI Platform and a UIL has been issued. Per step, a detailed description is given in the tables below.

3.1 SC1.3 MVP – eCMR lifecycle

The platform-managed eCMR lifecycle (preparation, pickup, delivery and closing). There is a single eCMR per version (V0/V1/V2); all actors receive the same attestation, and it is therefore not bound to a specific Business Wallet.

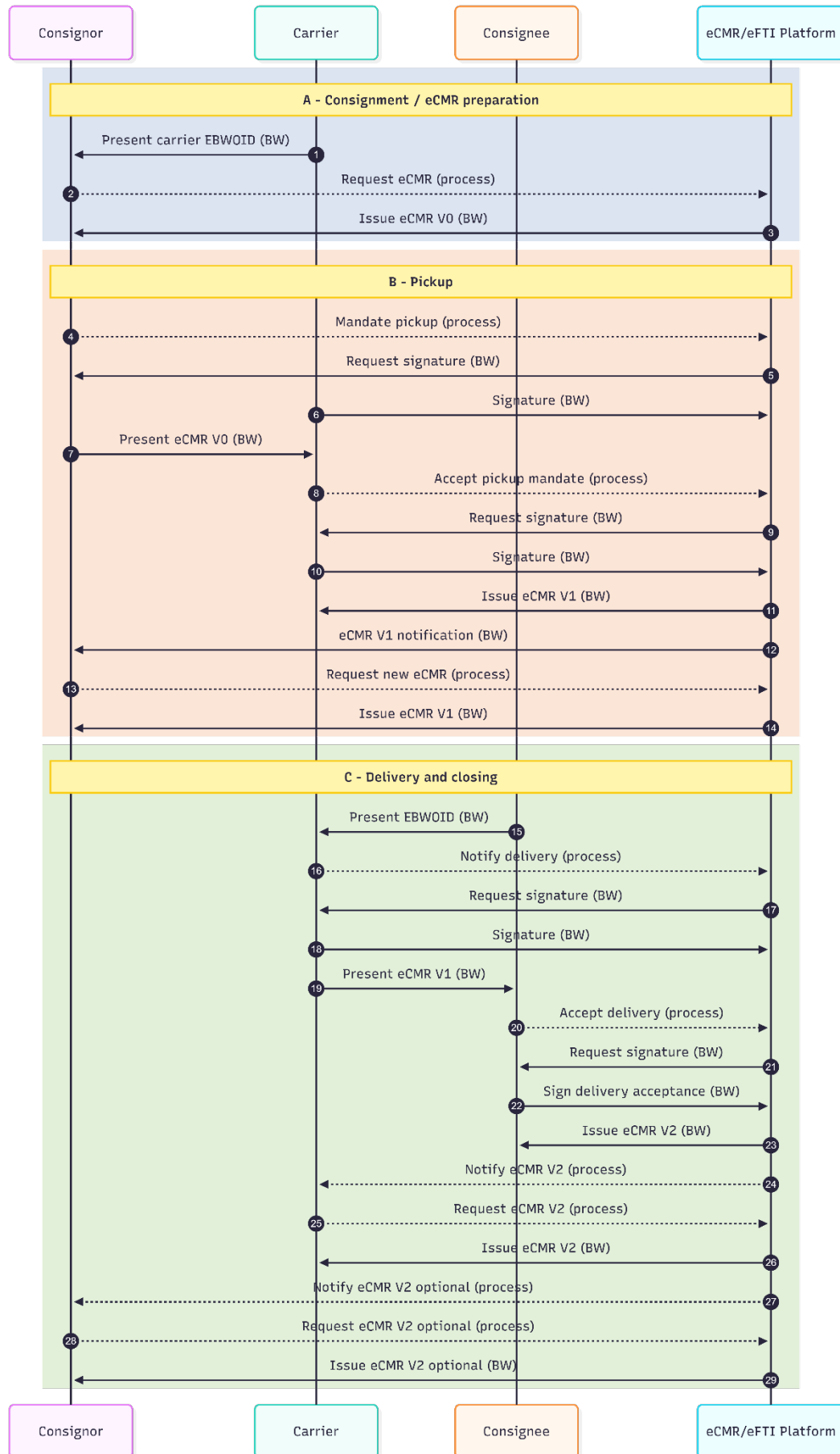


Figure 1 – SC1.3 (MVP): platform-managed eCMR lifecycle (preparation, pickup, delivery & closing) through the Business Wallet.

Legend — solid arrow = a step performed via/by the Business Wallet; dashed grey arrow = a platform-only / process step with no wallet involvement. Each message is also tagged (BW) or (process).

Step	Actor (from / to)	Interpretation or reference	Comment
Consignment / eCMR preparation			
1 Present carrier EBWID	Carrier / Consignor	The carrier presents its EBWID to be identified by the consignor.	
2 Request eCMR	Consignor / Platform	The platform creates the first version of the eCMR indicating the carrier and the consignor.	
3 Issue eCMR V0	Platform / Consignor	The platform issues the first version of the eCMR.	
Pickup			
4 Mandate pickup	Consignor / Platform	The consignor mandates the pickup, related to the current eCMR, using the identity provided by the carrier's EBWID.	
5 Request signature	Platform / Consignor	The platform asks the consignor to sign the pickup mandate.	
6 Mandate signature	Carrier / Platform	The pickup mandate is signed with the Business Wallet.	Check signer (consignor vs carrier).
7 Present eCMR V0	Consignor / Carrier	The consignor presents the eCMR V0 (step 3) to the carrier to connect to the platform and accept the pickup mandate.	
8 Accept pickup mandate	Carrier / Platform	The carrier connects to the platform to sign the pickup mandate initiated by the consignor, using the eCMR V0 to get the platform and consignment information.	
9 Request signature	Platform / Carrier	The platform asks the carrier for a signature to validate the mandate acceptance.	
10 Sign mandate	Carrier / Platform	The carrier uses its Business Wallet to sign the mandate acceptance.	

Step	Actor (from / to)	Interpretation or reference	Comment
11 Issue eCMR V1	Platform / Carrier	The platform issues a new version of the eCMR including the consignor and carrier signatures.	
12 eCMR V1 notification	Platform / Consignor	If enabled, the platform notifies the consignor that the new version is issued.	
13 Request new eCMR	Consignor / Platform	The consignor can request the new version. There is a single eCMR V1; all actors receive the same attestation, not bound to a specific Business Wallet.	
14 Issue eCMR V1	Platform / Consignor	The platform issues a 'copy' of the eCMR V1 to the consignor.	
Delivery & closing			
15 Present EBWOID	Consignee / Carrier	The consignee presents its EBWOID to be identified by the carrier.	
16 Notify delivery	Carrier / Platform	The carrier notifies the delivery, using the carrier identity from its EBWOID and the consignment information from the eCMR.	
17 Request signature	Platform / Carrier	The platform asks the carrier for a signature to validate the delivery notification.	
18 Sign delivery	Carrier / Platform	The carrier uses its Business Wallet to sign the delivery notification.	
19 Present eCMR V1	Carrier / Consignee	The carrier presents the eCMR V1 (step 11) to the consignee to connect to the platform and accept the delivery.	
20 Accept delivery	Consignee / Platform	The consignee connects to the platform and accepts the delivery, using the eCMR V1 for the platform and consignment information.	
21 Request signature	Platform / Consignee	The platform asks the consignee for a signature to validate the acceptance.	
22 Sign delivery acceptance	Consignee / Platform	The consignee uses its Business Wallet to sign the delivery acceptance.	
23 Issue eCMR V2	Platform / Consignee	The platform issues the eCMR V2 to the consignee, including both signatures.	
24 Notify eCMR V2	Platform / Carrier	If enabled, the platform notifies the carrier that a new version is issued.	

Step	Actor (from / to)	Interpretation or reference	Comment
25 Request eCMR V2	Carrier / Platform	The carrier can request the eCMR V2.	
26 Issue eCMR V2	Platform / Carrier	The platform issues a 'copy' of the eCMR V2 to the carrier (single version; same attestation for all actors, not bound to a specific Business Wallet).	
27 Notify eCMR V2	Platform / Consignor	If enabled, the platform notifies the consignor that a new version is issued.	Optional
28 Request eCMR V2	Consignor / Platform	The consignor can request the eCMR V2.	Optional
29 Issue eCMR V2	Platform / Consignor	The platform issues a 'copy' of the eCMR V2 to the consignor.	Optional

3.2 SC1.3bis MVP+ – control with or without the eFTI network

Roadside control combining the wallet path (EBWOID + eCMR attestation) with the eFTI network query (UIL via the national eFTI Gate to the eFTI Platform). The offline / wallet-only variant stops after the wallet verification.

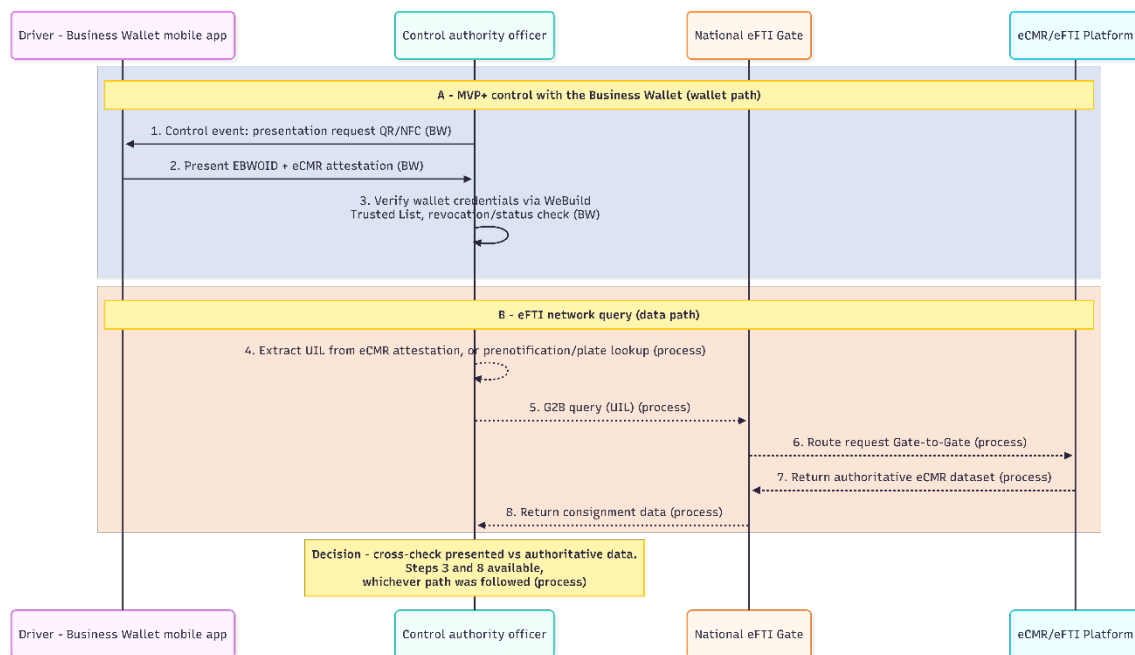


Figure 2 – SC1.3bis (MVP+): roadside control combining the wallet path (EBWOID + eCMR attestation) with the eFTI network query (UIL via the national eFTI Gate to the eFTI Platform).

Legend — solid arrow = a step performed via/by the Business Wallet; dashed grey arrow = a platform-only / process step with no wallet involvement. Each message is also tagged (BW) or (process).

Flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Roadside control – wallet path				
1. Control event	Competent authority (control officer)	The officer stops the vehicle / performs a control and initiates a presentation request via the proximity flow (QR code or NFC).	Officer authorization.	eFTI-only flow: step skipped, go directly to step 4 (Extract UIL).
2. Present credentials	Business Wallet / Competent authority (RP)	The driver presents the EBWOID and the eCMR attestation (incl. UIL).	Proximity flow, offline capable.	Sole-trader: carrier's own Business Wallet.
3. Verify wallet credentials	Competent authority / intermediary & Trusted List	The RP checks the carrier via the EBWOID, validates the eCMR attestation integrity using the EBWOID certificate, and verifies the trust chain via the WeBuild Trusted List.	Trusted List reachable; revocation / status check.	Offline / wallet-only flow stops after this step.
eFTI network query – data path				
4. Extract UIL	Competent authority	The RP reads the UIL from the eCMR attestation or obtains it from a prenotification / plate lookup in the eFTI-only flow.	–	
5. Query eFTI network	Competent authority / national eFTI Gate	Using the UIL, the authority issues a G2B query through its national eFTI Gate, which routes the request to the eFTI Platform holding the data (Gate-to-Gate).	Officer authorization; IR (EU) 2024/1942; Gate-to-Gate trust.	Cross-border: routed to a Gate / Platform in country A.
6. and 7.	eFTI routing	eFTI simplified mechanism flow is shown. eFTI EU network is not explained here.		
8. Retrieve authoritative data	eFTI Platform	The eFTI Platform returns the authoritative	Platform reachable.	

Flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
		consignment dataset (eCMR) for the UIL.		
Decision				
Cross-check	Competent authority	The RP cross-checks the data presented from the wallet against the authoritative eFTI data and performs the control.	Steps 3 and 8 available (whichever path — wallet or eFTI network — was followed).	Handover: discrepancy recorded (linking optional).

Other checks performed by the authority at the same time (weight, ADR, driving times, permits) are out of scope of this scenario.

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
User of Wallet	Drivers and companies on behalf of eFTI Platform operators (see 4.3). Other candidate carriers: CEVA group, Ybil OU (already joined the SC1 group, see SC1.1).	BE, DE, EE, ES, FR, NL
Authentic sources	EBWOID issued by WP4 and/or other UC (those partners are not in SC1). Registradores (ES), Infogreffe (FR), KvK (NL); BE/DE/EE TBD or covered by a WP4-created register / QTSP.	BE, DE, EE, ES, FR, NL
Relying party (control)	Competent authority – a national road-transport enforcement authority performing the control. In the pilot it may be simulated by an SC1 partner acting in that role, or a real enforcement body (tbc).	NL, EE, ES, FR (tbc)
Consignment issuers / eCMR / eFTI Platform operators	Provide the consignment dataset and the UIL. Pionira (BE), Ybil OU (EE), Fieldeas (ES), CEVA (FR, tbc).	BE, EE, ES, FR
eFTI Gate operator	National eFTI Gate(s) used for the G2B / Gate-to-Gate query.	FR, EE, NL, ES (tbc)

Primary role	UC partner Name	Country
Intermediary	Optional intermediary service between the relying party and the wallet / eFTI network (as in SC1.1 and SC1.2).	

4.2 Additional roles and partners

Partners that primarily work in WP4 and participate in piloting this scenario. Section 3 of the Stock Taking document can be used as a basis.

Primary role	UC partner Name	Country	Wallet
Wallet provider	Digidentity, Credenco, Sphereon (tbc)	NL, DE	BW
eFTI Gate provider	National eFTI Gate operator(s)	FR, EE, LT, DE, NL	–
PID Provider	Citizens registers (FR, EE, BE, ES, NL, DE) – optional, sole-trader variation only		
Trusted list registrar	TBD – input expected from WP4		
EAA provider	The eCMR/eFTI platform issues the eCMR attestation (per rulebook)		
QES provider	In MVP+		

4.3 Target country combinations

The choice of holders (companies and drivers) will target countries near the relying parties and will be made when concrete things are available to be shown. Cross-border combinations are made by choosing a carrier in a different country than the control authority.

Note: the country sets targeted for SC1.3 (4.1) do not need to match those used in SC1.2 — the two scenarios are pilotable independently and may involve different partner combinations, even though they are logically sequential in the overall transport chain.

SC1.3 (MVP).

Cross-combinations between the countries of the eCMR/eFTI platforms involved: at least one company per country will ship / pick up / deliver / receive the goods from another company (brought by another eCMR/eFTI platform). At least 3 combinations are expected, and the number could be up to 10. Countries expected: BE, EE, ES and FR

SC1.3bis (MVP+).

RP country \ Issuing	BE	DE	ES	FR	NL	EE
NL	X	X		X	X	X
ES			X	X		
FR	X	X		X	X	X
EE		X		X		X

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners) or are to be provided by other use cases or working groups. The details of each attestation created within the scenario are described in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For Countries	Requirements
EBWOID	European Business wallet owner identification (carrier).	WP4 PID/LPID group	BE, DE, ES, FR, NL, EE	Carries the technical identity used to sign the carrier's attestations.
PID	Personal ID – only for the sole-trader variation.	WP4 PID/LPID group	FR, BE, NL, DE, EE, ES	Optional in this scenario.
UIL	Unique Identification Link – eFTI network reference to the consignment	eFTI Platform	tbc	Per Reg. (EU) 2020/1056 and IR (EU) 2024/1942.

5.3 Created attestations in the scenario

The scenario uses one created attestation: the eCMR attestation (rulebook v1.0).

Attestation name	Short description	Applicable standards	domain
eCMR attestation	Electronic Road Consignment Note carried in the Business Wallet. Based on the eCMR data model with an added wallet envelope object (issuer_id, ecmr_attestation_id) that links the credential to the eFTI Platform record / UIL. The eCMR attestation and the eFTI QR code/UIL are treated as a single credential; used by the control officer together with the EBWOID to verify the consignment in transit.	UN/CEFACT D24A WeBuild attestation v1.0.	e-CMR (19.12.2024); eCMR rulebook

Open points still to be checked with the rulebook design:

- Proximity-flow format (e.g. mdoc) for the offline control.
- Cryptographic binding of the eCMR attestation to the Business Wallet and verifiable issuance by the eCMR/eFTI platform.
- Integrity matching between the eCMR attestation envelope and the authoritative eFTI Platform record (via the UIL).
- eCMR–eFTI definitions and data-model differences in the semantic model: the SD-JWT format is not supported by WP4 (the semantic model cannot be used).

Annex 1 – Requirements for scenario roles

This annex lists the main functional / organizational / technical requirements for each role in the scenario.

Primary role	Specific requirement
User of Wallet	a) Holds a Business Wallet with the EBWOID and the eCMR attestation.
Authentic sources	b) Business registers will issue an EBWOID (or a QTSP does so).
Relying party (control)	
eCMR / eFTI Platform	c) Has interface with Business Wallet. d) Will hold the consignment dataset and issues a UIL per consignment. e) Transmits the consignment data on a valid UIL query.
eFTI Gate (MVP+)	f) Routes eCMR query from control to eFTI platform g) Routes the eFTI dataset query between other eFTI gates.
Intermediary	
Wallet provider	h) will provide a business wallet that includes the EBWOID of that company i) will provide a proximity interface on mobile devices to the business wallet. j) will authorize the company to revoke the eCmr attestation k) will support mdoc format for that attestation l) will make the wallet usable offline m) will prevent another person to use the personal wallet. Note: no need of a certified Wallet (PID & LOA high not needed)
Trusted list registrar	
EAA provider	n) The eCMR platform issues the eCMR attestation.
QES provider (MVP+)	

WE BUILD consortium

Specification Scenario 1 – Enrolment and trusted contracting

WP2 – SC1 – Authentication and access for transport

Date : 28/07/2026
Version : 0.8 (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)
Status : Draft (Draft, for review, reviewed, final)

Index

Introduction	3
<i>Objectives of this document</i>	<i>3</i>
<i>Scenario introduction</i>	<i>3</i>
Scenario specification.....	3
<i>Introduction.....</i>	<i>3</i>
<i>Summary of scenario variations:.....</i>	<i>4</i>
<i>Preparation before the KYB.....</i>	<i>4</i>
<i>Performing a KYB with the PCS.</i>	<i>5</i>
<i>SSO and Mandating employees of the carrier.....</i>	<i>5</i>
<i>Scenario pre-conditions.....</i>	<i>7</i>
<i>Scenario main flows</i>	<i>8</i>
Variation B, Sole trader: KYB	9
Variation A: KYB, mandate and SSO of the employee.....	9
<i>Scenario additional flows</i>	<i>10</i>
<i>Challenges and barriers.....</i>	<i>11</i>
<i>Working Assumptions</i>	<i>11</i>
Detailed scenario flow.....	12
<i>Scenario A: KYB, mandate and SSO of the employee managed by a Business Wallet.</i>	<i>12</i>
Roles and participants	16
<i>Scenario roles and participants.....</i>	<i>16</i>
<i>Additional roles and partners.....</i>	<i>17</i>
<i>Target country combinations</i>	<i>17</i>
<i>Requirements</i>	<i>18</i>
Attestations	19
<i>Introduction.....</i>	<i>19</i>
<i>Attestations to be provided by other UCs/WGs/scenarios.....</i>	<i>19</i>
<i>Created attestations in the scenario.</i>	<i>20</i>
Annex 1 – Requirements for scenario roles.....	21

Introduction

Objectives of this document

This document describes the details of scenario 1, as part of use case SC1 in work package WP2 in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting. The final chapter explains what will be learned from the scenario.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

Scenario introduction

Registration of a transportation company on a seaport's Port Community System, submission of the legal entity's ID and attributes via a Business Wallet activated by a legal representative. Registration of a company employee and issuance of mandates to this employee. Signing of a contract in MVP+.

- Use case of a sole trader using a Natural Person Wallet being covered.
- Pilot will cover foreign carrier enterprises onboarding on the Rotterdam PCS system using a Business Wallet.

Scenario specification

Introduction

A port facility must certify all companies operating within its premises, for reasons of safety and economic efficiency. These issues are particularly critical given the high volumes and performance requirements inherent to the industry.

The pilot program will focus on the many transportation companies (Carriers) operating in seaports; the goal is to streamline registration procedures, improve the quality of the information collected, and enable these companies to identify their employees authorized to interact with the Port Community System (PCS).

Carriers will be able to complete their registration procedures online and submit their supporting documents in digital format. This will save a great deal of time and effort and reduce the burden of paper handling in most of the PCS systems. Even for advanced PCS like Portbase the biggest friction in the current process is the ID verification of the legal representative of the carrier e.g. to operate in the port, she/he must perform at least 4 to 5 different ID verification processes (Portbase PCS, Secure Logistics, Municipality, Terminals).

This scenario consists of two consecutive steps:

1. Execute a Know Your Business partner (KYB) operation to onboard the Carrier company on the PCS. That step is the common ground for the relying parties.
2. Using the business wallet to mandate employees of the carrier and perform Single Sign On (SSO) access of PCS.

The scenario is dedicated to carrier company (larger than a sole trader) that uses its business wallet for the KYB process and uses the business wallet for authorization and SSO.

Due to different populations of carrier enterprise we are considering a variation of the pilot scenario: the case of sole trader using his personal wallet to complete the KYB process and perform an SSO on the PCS

The scenario will include an optional flow to cope with more complex cases for example when other companies own a company and the business register of the company has no natural person who can represent the company.

Summary of scenario variations:

Scenario variation.	Wallet holder & Wallet type	KYB step	Mandate & SSO step (optional)
A	A Carrier company using a Business Wallet.	KYB from Business Wallet performed by legal person.	Performed by Business Wallet (optionally assisted by professional wallet).
B	Sole trader using Personal Wallet	KYB from personal wallet.	Perform a SSO with his/her personal Wallet..

Preparation before the KYB

These following steps are integrated in the experimentation scenario and will be demonstrated.

All scenario variations: PID issuance

A legal representative of the transport company or the sole trader must contact a PID issuing authority in their country of residence to obtain a PID, which she/he will store in her/his personal EUDI-Wallet.

Variation B: EBWORLD issuance

The sole trader contacts a business registry to issue an EBWORLD associated with an EUCC wallet in her/his personal wallet.

Then the sole trader asks a tax authority to issue a "VAT ID certificate" to his personal wallet.

Variations A: EBWORLD issuance

The legal representative must then contact a business registry to issue an EBWORLD associated with an EUCC and an UBO in a Business Wallet linked to the company.

Later a Business Wallet user (only a legal representative or a dedicated Business Wallet Administrator) can then have a "VAT ID certificate" issued to the Business Wallet by a tax authority of the country that issued the EBWORLD.

MVP+

As an optional feature, in MVP+ it will be allowed to connect with administrative authorities to generate the following certificates in the Business Wallet:

- LEI, Legal Entity Identifier issued by GLEIF.
- IBAN, issued by a financial operator
- Peppol ID, issuer to be defined
- EORI, Economic Operator Registration Identification issued by custom admin.
- UBO Ultimate Beneficiary Owner.

Performing a KYB with the PCS.

In order to open a business relation with the port's PCS department, the company must complete a KYB procedure on the PCS portal. Using the business wallet, an authorized user must provide the EBWOID, the EUCC, and the VAT ID certificate. This will proceed via intermediary services provided by a third-party company.

Then, the legal representative registers the company to one or more of the PCS services, ready to sign a contract between the company and PCS authorities.

SSO and Mandating employees of the carrier.

To use PCS services, the transportation company must identify its employees and, if necessary, issue them with mandates to perform specific tasks. First, a legal representative of the company will be granted a mandate of "Business Wallet Administrator"; This administrator needs to onboard the employee to allow to SSO on the PCS and to request an Employee Mandate Attestation. In a second step this Business wallet administrator needs to validate the issuance of an Employee Mandate.

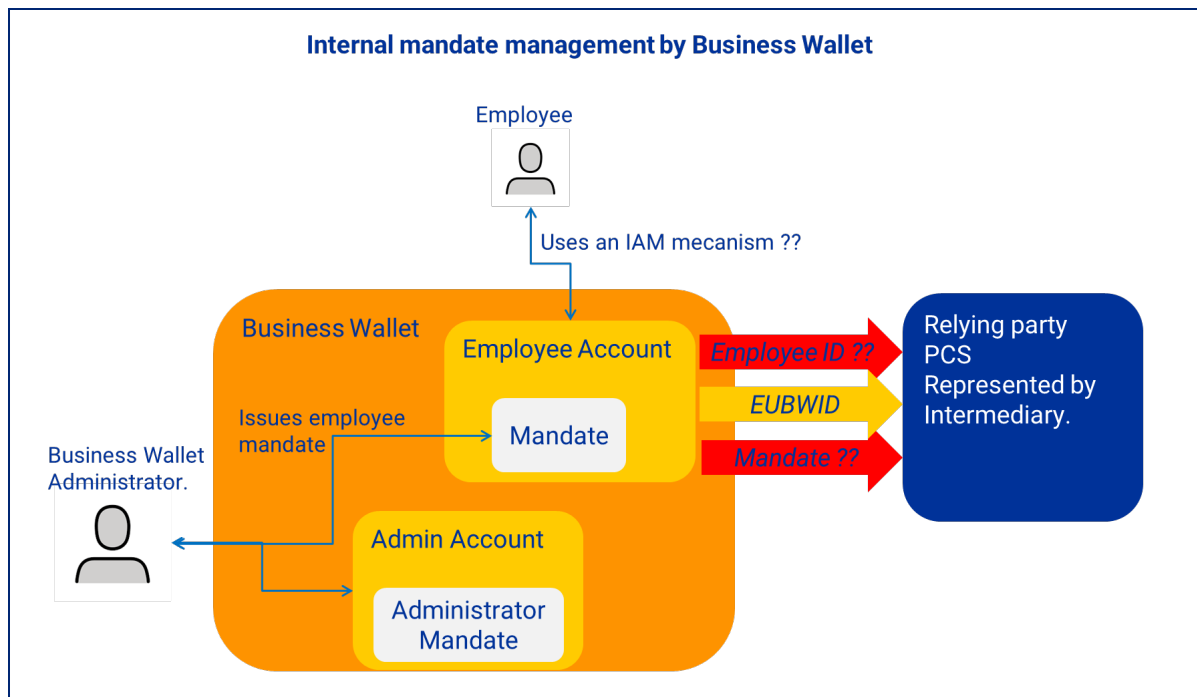
When interacting with the PCS the employee will be asked to identify himself (SSO) and present its mandate. When accessing the SSO of the PCS the employee needs to be identified, the minimum requirement could be a business mail address.

There are two technical options to perform the SSO and issue this mandate:

Internal process within the business wallet: An authorized person (the Business Wallet Administrator) identifies the employees and allow them to use the Business Wallet via an account and has the business wallet issue "Employee Mandate Attestation" (POE) stored in the employee user space, the mandate attestation can be presented towards a Relying Party like PCS by the employee. The attestation can be withdrawn by the BW Administrator.

To be clarified with architecture and wallet editors teams(WP4). In this mode, the employees and administrator will have an account open in the Business Wallet, this account will contain the mandates of the employee/administrators. The access control to these accounts of the Business Wallet must be defined. During the exchange Business Wallet / Relying Party, the identification of the employee and the mandate presentation need to be specified.

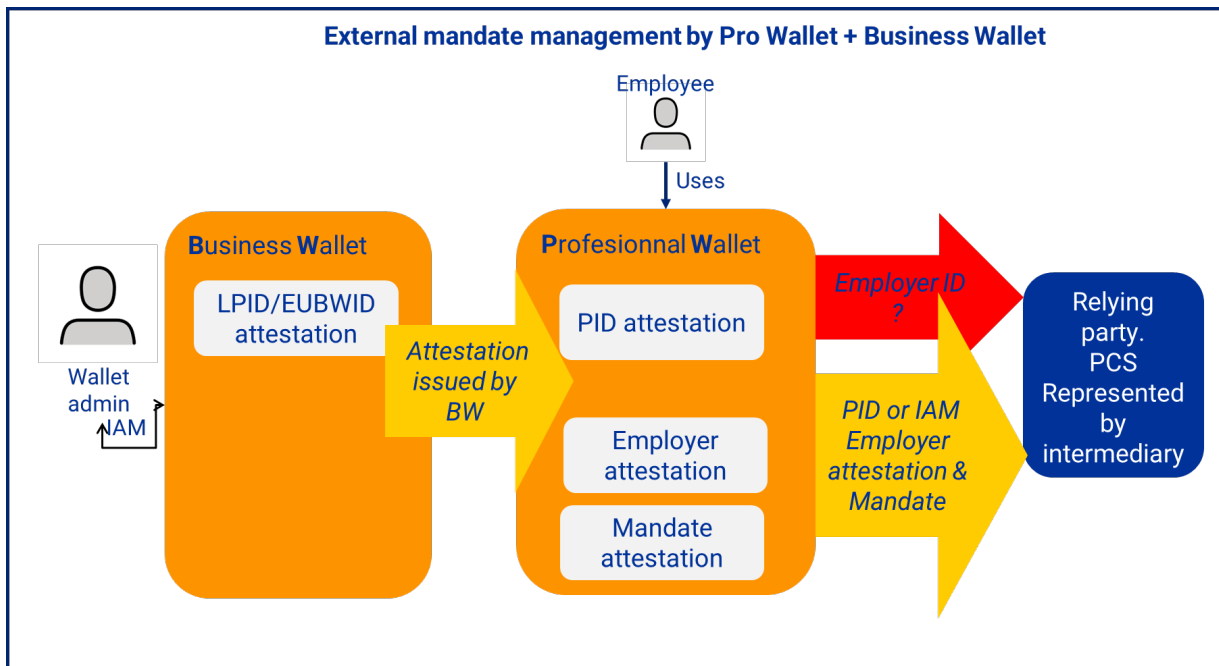
The internal mode is presented in the following figure:



External process will use the employee's personal/professional wallet in conjunction with the business wallet. The same authorized person identifies the employees and has the business wallet to issue an Employee Mandate attestations, which are stored in the employee personal/professional wallet.

To be validated with architecture team. The Professional Wallet offers the same features as a Personal Wallet but is designed for professional use. It is typically issued by the employer and managed by the employee on her/his mobile phone. We should not enforce employees to use their personal wallet for business interactions.

The external management of mandate via a professional wallet is presented in the following figure:



To be validated with architecture team. The mechanism to issue an attestation from the business wallet to the personal/professional wallet of the employee need to be specified. In this case the identification of the employee will be naturally done by presentation of the PID or by IAM mechanism, but the question arises: “how will be identified the enterprise” because its EBWID cannot be stored in the personal/professional wallet of the employee. It may be derived from the digital signature of the employer or mandate attestation.

Will it be compulsory to personnal/professionnal to include an IAM mechanism?

Note: In the Netherlands, it is not allowed to use the PID (BSN). For the Professional Wallet, the same ID could be used (above internal process).

Scenario pre-conditions

Prerequisite to the scenario variation B sole trader using a personal Wallet:

- The sole trader downloads a valid wallet (certified)

- The sole trader contacts a PID-issuing entity. They follow the enrolment procedure required by the PID issuer and load their PID into their EUIDAS personal wallet.
- The carrier entity is listed in a business register, and the sole trader is listed as a legal representative of the carrier.
- The sole trader presents his/her PID and asks the business register to issue an EB-WOID/EUCC attestation in her/his personal wallet.
- PCS Service Provider is registered as a relying party for personal wallet, able to request PID, EBWOID
- There is an agreement of the PCS owner with an intermediary operator.
- The intermediary actor is registered as an Intermediary for Business Wallets.

Prerequisite to the scenario variations A, a carrier company using a Business Wallet.

- A legal representative of a transport company has activated a certified personal wallet and as contacted a PID-issuing entity. They follow the enrolment procedure required by the PID issuer and load their PID into their EUIDAS personal wallet.
- The carrier entity is listed in a business register, and the legal representative is listed as a legal representative of the carrier.
- Carrier procured a certified business wallet solution and have it installed and running.
- PCS Service Provider is registered as a relying party for Business Wallets, allowed to request presentation of EBWOID, EUCC and VAT ID certificate.
- There is an agreement of the PCS owner with an intermediary operator.
- The intermediary actor is registered as an Intermediary for Business Wallets.

Scenario main flows

Actors

The issuing of a PID is kept outside of the scenario as it is a prerequisite.

One need an EBWOID as a Pub-EAA provider, it is assumed that this issuer will be able to issue in the same request: EBWOID, EUCC.

VAT ID Certificate could be issued by a tax administration as a PUB-EAA provider or by a QTSP provider from a tax administration physical document.

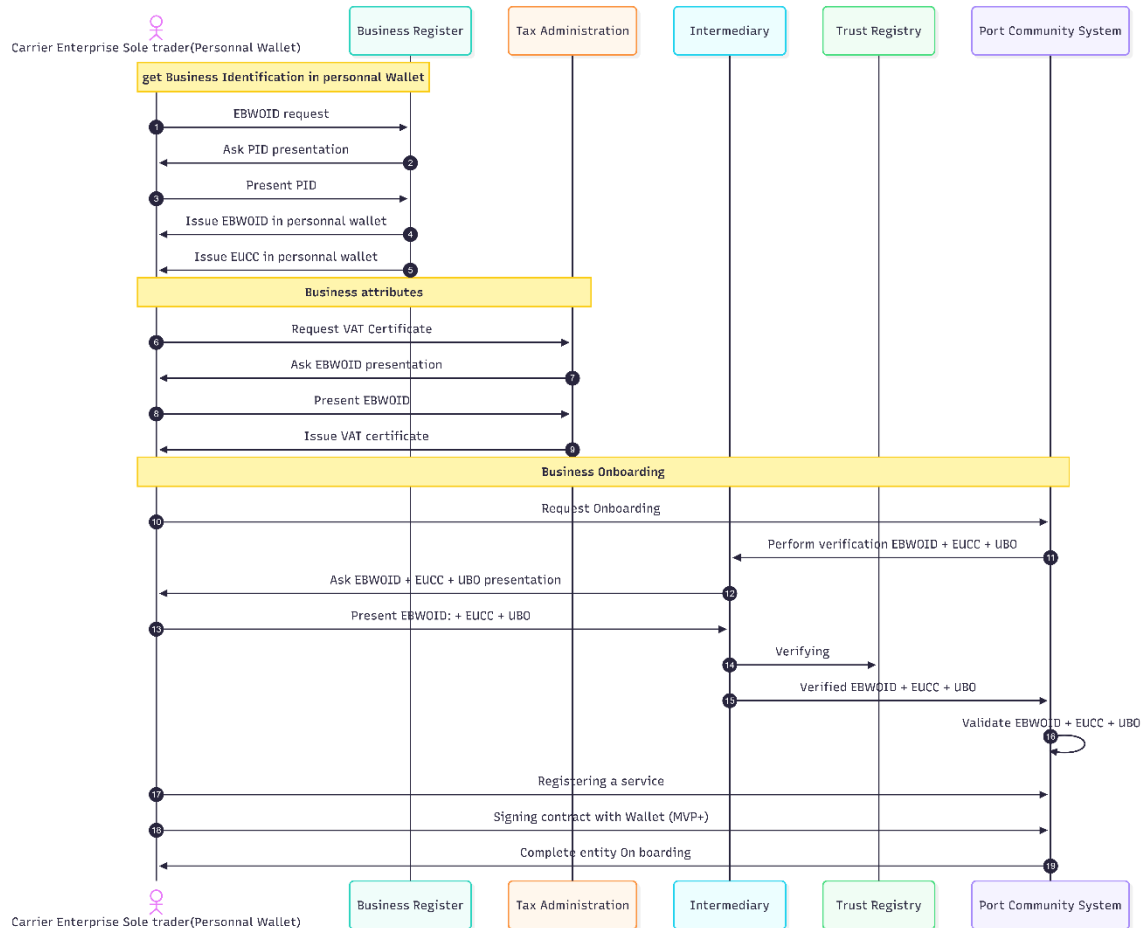
In this use case the relying party (the Port Community System) will rely on an Intermediary service.

The Business Wallet acts as EAA issuer (in behalf of the Carrier), for Employee Mandate attestation.

The pilot framework will be cross border:

- The relying parties are based in the Netherlands and in Spain (tbc).
- The Enterprise, EBWOID issuers, the PID issuers and PUB-EAA will be located in NL, DE, ES or FR.

Variation B, Sole trader: KYB



Variation B: Sole trader

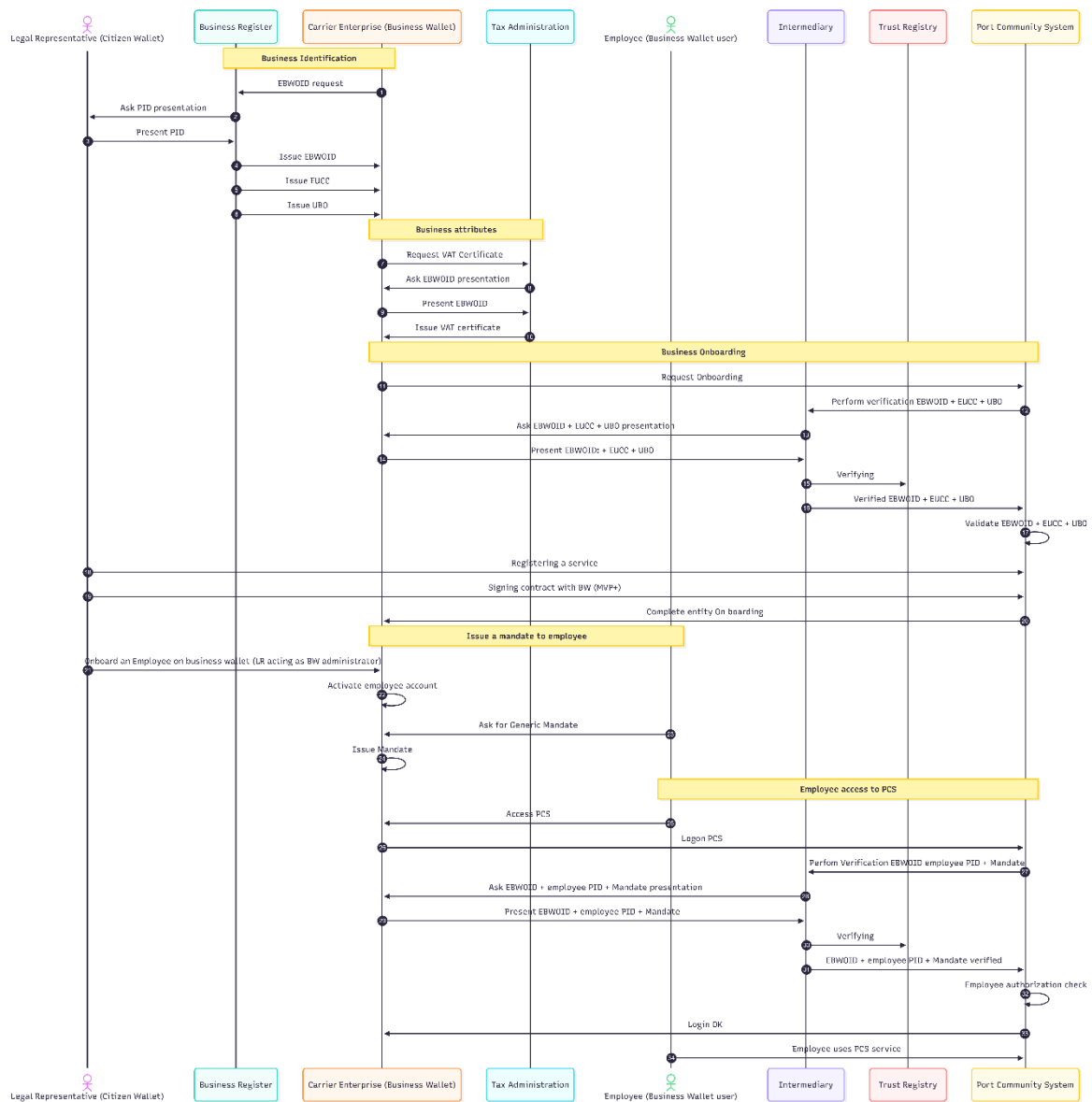
The sole trader case using either an eIDAS wallet or a simplified business wallet will be considered. The WP4 architecture group will define which wallet architecture will be used.

The sole trader is onboarding her/his business activity by performing a KYB. Later the Sole trader can interact with PCS to perform SSO with her/his wallet.

Variation A: KYB, mandate and SSO of the employee.

A Carrier Enterprise onboard on PCS via KYB using its Business Wallet. Later the Carrier Enterprise issues mandates and allow Employees to SSO on the PCS by using the Business Wallet or a combination of Business Wallet and Professional Wallet.

SSO of the employee managed by a **business wallet**.



Scenario additional flows

Flows	Short description
Variation A: A carrier company Using business wallet only.	A Carrier Enterprise onboard on PCS via KYB using its Business Wallet. Later the Carrier Enterprise issues mandates and allow Employees to SSO on the PCS by using the Business Wallet or a combination of Business Wallet and Professionnal Wallet

Variation B : Sole trader	The sole trader case using either an eIDAS personal wallet or a simplified business wallet will be considered. The WP4 architecture group will define which wallet architecture will be used. We will align on BU1 recommendations on the sole trader. The sole trader is onboarding her/his business activity by performing a KYB. Later the Sole trader can interact with PCS to perform SSO into the PCS with her/his wallet.
Exceptions	No exceptions.

Challenges and barriers

Partner resource availability and commitment – Partners may lack sustained commitment or available technical/business resources throughout the pilot, slowing deliverables or causing knowledge gaps.

Recruiting Carrier enterprises as wallet Holders for the production phase. CEVA group and Ybil OÜ joined the SC1 Group who is a strong Carrier active in France, this is a nice opportunity. Since we are looking for three different carrier companies we will need to recruit other carriers, some selection will be made within the thousands of clients of the relying parties (companies accessing to Harbours).

Working Assumptions

See expectations in scenario description in previous chapters.

Detailed scenario flow

Scenario A: KYB, mandate and SSO of the employee managed by a Business Wallet.

The variations B are listed as variations in this table.

Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Download Business Wallet.	Legal Representative.	1.The Legal Representative download a Business Wallet and install it. Wallet generates wallet keys and binds device.	The Legal Representative has already downloaded an EUDI Wallet and has loaded the PID from an authentic source.	Variation for sole trader they will be use a eIDAS personal Wallet instead of Business Wallet. This defined by the architecture WP4.
Request and Issue attestations for KYB.	Legal Representative.	2. The legal representative request the attestations for the Carrier Enterprise. Attestations are: • EBWID, • EUCC, • UBO (moved to MVP+)	The Legal Representative use the Business Wallet or the Business Register Interface to complete this request. We need to get input of WP4 PID-LPID Group. Support from BU2 EUCC will be requested.	For sole trader it will be the sole trader her/himself.
	Business Register	3.The business register request presentation of Legal Representative PID.	The Legal Representative has obtained a PID from authentic source.	
	Legal representative.	4.The Legal Representative presents from the his/her eIDAS personal Wallet the PID.		
	Business Register.	5.Business Register verify if request is issued by legal representative.		
	Business Register.	6.Business Register Issues attestations in Business Wallet.	If validation 5 is successful. And Business Register is listed in Trusted List.	
	Business Wallet	7.The Business Wallet stores the attestations and bind them with the device.		See Sole Trader Variation. The WP4 architecture group will define the kind

Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
				of personal/business wallet used.
Request VAT certificate and issuance.	Business Wallet/Legal Representative.	8.Request VAT Id Certificate to Tax Administration for Carrier Enterprise.	There is a dependency with BU3 work package who is in charge of those attestations.	See Sole Trader Variation.
	TAX Administration Issuer.	9.Request EBWOID presentation to identify the Carrier Enterprise.		
	Business Wallet/Legal Representative.	10.Present to the Tax Administration Issuer the EBWOID of Carrier Enterprise.		
	Tax Administration Issuer.	11.Query the VAT authentic database and push the VAT Id Certificate to the Business Wallet f	Tax Administration must be listed in Trusted List. Or the VAT Id certificate is issued by a QTSP.	
Onboarding on PCS.	Legal Representative.	12.Ask for onboarding of the Carrier Enterprise on the PCS IT system.	We need to synchronize with BU1, it is formally a KYB process.	
	PCS Online service.	13.PCS ask to intermediary to validate onboarding attestations: EBWOID, EUCC, UBO (moved to MVP+).	Support from WP4 architecture is requested, on the Intermediary service.	
	Intermediary.	14. Requires presentation of attestations:		
	Business Wallet/Legal Representative.	15. Presentation by the Business Wallet of the requested attestations to Intermediary.		
	Intermediary.	16.Verification by Intermediary of status/revocation of issuer to Trusted Registry.		
	Intermediary.	17. Intermediary return verification status to the PCS.		
	PCS	18. Validate datasets extracted from Attestation.	Only of the Intermediary validation is OK: integrity	

Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
			of attestations and validation of issuing authorities.	
	PCS	19. Validate the KYB/Onboarding of the Carrier Enterprise to the Legal Representative.	Also, a check is required if the company is already a PCS customer or not. The EUID within the EB-WOID is source. For non Dutch organisations there's no easy mapping towards the currently available data within the PCS to perform this check. Most likely will be a generic issue for most Relying Parties.	
	Legal Representative.	20. Registering the Carrier Enterprise to PCS.		
Issue Mandates to Employee.	Legal representative.	21. Assign a Business Wallet Administrator and give him Access Rights. The Wallet administrator Onboards Employee on the business Wallet.		
	Business Wallet administrator.	22. Activate a business wallet account for the employee.		
	Employee	23. Ask mandates to Business Wallet	Here we need support from WP4 Architecture, If the Business wallet issues the mandate, it will an EAA attestation, who will be the issuing authority the Carrier Enterprise?	A variation possible is to store the mandate in a professional Wallet. We are waiting from WP4-Wallet group and architecture to make a decision on these variations.
	Business Wallet/Administrator.	24. Validate the request and issue the mandate to the Business Wallet		Variation: manage mandate from Professional Wallet instead of Business Wallet.

Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Employee access to PCS.	Employee.	25. Logon to PCS		For sole trader case the logon PCS will be done from the personal wallet.
	Business Wallet	26. Initiate the LOGON the PCS.		
	PCS	27. Ask to intermediary to validate, PID, EBWOID and Mandate.		
	Intermediary.	28. Require presentation of PID, EBWOID and Mandate to professional Wallet.		
	Professional Wallet.	29. Present PID, EBWOID and mandate to Intermediary.		Variation: following WP4 recommendation, manage mandate from Business Wallet instead of professional Wallet.
	Intermediary.	30. Validate with Trust Registry the attestations.	We need WP4 support what will be trust registry for an attestation issued by a Business Wallet.	
	Intermediary.	31. Intermediary return verification status to the PCS.		
	PCS	32. Validate the Employee Logon.		
	PCS	33. Validate logon to Employee.		

Roles and participants

Scenario roles and participants

Primary role	UC partner Name	Country
1. User of EUDI Wallet	The user of the EUDI wallet may be of two kinds: 1. The legal representatives of Carrier Enterprises. The legal representative will be a user of the Business Wallet and will perform a KYB to onboard the Carrier enterprise on a Port Community System. 2. The employee of Carrier Enterprises. IN scenario SC1.1 variation C the employee can use a Professional Wallet (variation of the EUDI Wallet) to interact with the PCS. Activ on FR, NL and SP Employee of CEVA Group can be user of the EUDI personal wallet. We plan to recruit carrier already using the PortBase services.	
1 Bis User of Business Wallet.	The user of the Business Wallet will be Carrier enterprise willing to onboard and exchange on the Port Community System of a Port. Three kinds of Business wallet will be experimented: 1. Sole Trader. 2. Carrier enterprise.FR, administrators and drivers from CEVA Group. 3. NL we plan to recruit carriers already using Port-Base serices.	
2. Authentic sources	a) Citizens Registers will Issue PID for Legal representatives, or Employee. b) Business registers will issue EBWOID, EUCC attestations for Carrier companies. c) Tax Authorities will issue VAT Id certificates to Carrier Enterprises. TAX Authorities from NL will be involved. For EBWOID issuing authorities could be identified in 6 countries listed (WP4 communication). For EUCC issuing; exchange will be organized with KVK (NL), Infogreffe (FR), Bundesanzeiger (DE), Registradores (ES). For VAT Id certificates; Dutch Tax agency (NL), Datev (DE).	FR, ES, NL, DE
3. Relying party	The Relying Parties will be the Port Community System form a Port Authority.	NL, ES

Primary role	UC partner Name	Country
	PortBase the PCS operator of Rotterdam Harbour (NL), plan to be a 1st relying party. Portic the PCS of Barcelona Harbour (SP) would be a 2nd Relying Party (to be confirmed) An Cargo fresh market place is interested to join the experimentation. The platform is called B2PWEB it is base in FR. It will be proposed to Haropa Port (FR) to join the experimentation.	
4. Intermediary	PortBase will use Intermediary service, they will be connected to Anoigo. Portic way of working needs to be clarified more likely the enterprise ITSME (BL) IN groupe developed intermediary services and can act as intermediary service provider	

Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	BW (Credenco ²) (BW, NW) Digidentity (BW) Spherity.(tbc) (NW) IN Groupe	NL NL DE	
2. PID Provider	Identical to EBWOID providers. Citizens registers from, FR, ES, NL, DE will be involved to deliver an identity to legal representatives to Carrier Enterprises.		
3. Trusted list registrar	TBD We are waiting input from WP4 group.		
4. QEAA provider			
5. Pub-EAA provider			
6. EAA provider	Employer, the Business Wallet users will issue mandate and attestation to their employees.		
7. QES provider	In MVP+		

Target country combinations

Issuing country

Relying Party country		NL	ES	FR			
	NL(						
	ES						
	FR (if Haropa or B2PWEB joins)						
	...						

Yellow cells: if too many attestations need to be faked for a combination, then that combination could be abandoned.

Requirements

The main requirements for each of the involved roles are included as an Annex.

Attestations

Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners) or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

Attestations to be provided by other UCs/WGs/scenarios.

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Personal ID attestation. Citizen ID attestation.	WP4 PID/LPID Group.	FR, , NL, DE, , ES.	Used to identify the legal representative of Carrier Enterprise. Identification of Wallet Users. Provided by WP4 PID/LPID group and BU1
EBWOID	Legal Person identification.	WP4 PID/LPID Group.	FR, NL, DE, ES.	Provided by WP4 PID/LPID group and BU1
EUCC	EU Company Certificates.	BU2	FR, NL, DE, ES.	Provided by BU2
VAT Id Certificate	VAT Id Certificate	BU3	NL, others TBD.	
POE	Power Of Employee	BU4	Issued by Carrier wallet holder.	Formerly identified as Employer attestation. The POE will attest a work agreement between the employer (Issuer) and the employee (wallet user).
	MVP+ attestations			
LEI.	Legal Entity Identifier issued by the GLEIF			
IBAN	issued by a financial operator			

EORI	Economic Operator Registration Identification issued by custom admin			
------	--	--	--	--

Created attestations in the scenario.

Attestation name	Short description	For Countries	Applicable domain standards
Peppol ID	he Peppol Id Attestation (PA) is an attestation that proves that a legal entity participates in the Peppol ecosystem within one or more Peppol business domains and provides the Peppol Participant Identifier used for addressing and capability discovery	To be defined with the SC1.1bis mvp+ scenario	

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of EUDI Wallet	a. CEVA Group (FR)
	b.
	c.
2. Authentic sources	a. Bundesanziger (DE)
	b. Greffe des tribunaux de commerce (FR)
	c. KVK (NL)
3. Relying party	a. PortBase (NL)
	b. Portic (SP)
	c. B2PWEB (FR)
4. Intermediary	a. ANOIGO (NL)
	b. ITSME (BE)
	c. IN Groupe (FR)
5. EUDI Wallet provider	a. Credenkeno (NL)
	b. Digidentity (NL)
	c. Spherity (DE)
6. PID Provider	a. FIN (FR)
	b. (DE)
	c. (NL) (SP)
7. Trusted list registrar	a. TBD (NL)
	b. TBD (FR)
	c. TBD (GE)
8. QEAA provider	a. BUndesanziger
	b. Greffe des tribunaux de commerce
	c.
9. Pub-EAA provider	a.
	b.
	c.
10. EAA provider	a. POE Issuer, Carrier employers
	b.
	c.
11. QES provider	a. To replace VAT-ID issuer

	b.
	c.

WE BUILD consortium

Specification Scenario SC1.2 – Identify and security access

WP2 – SC1 – Authentication and access for transport

Date : 09/07/2026
Version : 1.0
Status : final

Index

1	Introduction	3
1.1	<i>Objectives of this document.....</i>	3
1.2	<i>Scenario introduction.....</i>	3
2	Scenario specification.....	5
2.1	<i>Introduction</i>	5
2.2	<i>Scenario pre-conditions</i>	6
2.3	<i>Scenario main flow</i>	6
2.4	<i>Scenario alternate flow.....</i>	7
2.5	<i>Challenges and barriers (fast and secured).....</i>	7
2.6	<i>Working Assumptions</i>	8
3	Detailed scenario flow.....	9
4	Roles and participants	10
4.1	<i>Scenario roles and participants.....</i>	10
4.2	<i>Additional roles and partners</i>	10
4.3	<i>Target country combinations.....</i>	11
4.4	<i>Requirements.....</i>	11
5	Attestations	12
5.1	<i>Introduction</i>	12
5.2	<i>Attestations to be provided by other UCs/WGs/scenarios.....</i>	12
5.3	<i>Created attestations in the scenario</i>	12
	Annex 1 – Requirements for scenario roles.....	13

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario SC1.2 “Identify and security access”, as part of use case SC1 “Authentication & access for transport” in work package 2 “in the WE BUILD consortium. The document provides detailed information on the processes to be piloted, attestations to be used and partners that are involved in creating solutions and piloting.

The document is the result of the Specification Phase of the WE BUILD LSP and is an important step towards developing the solutions needed for piloting.

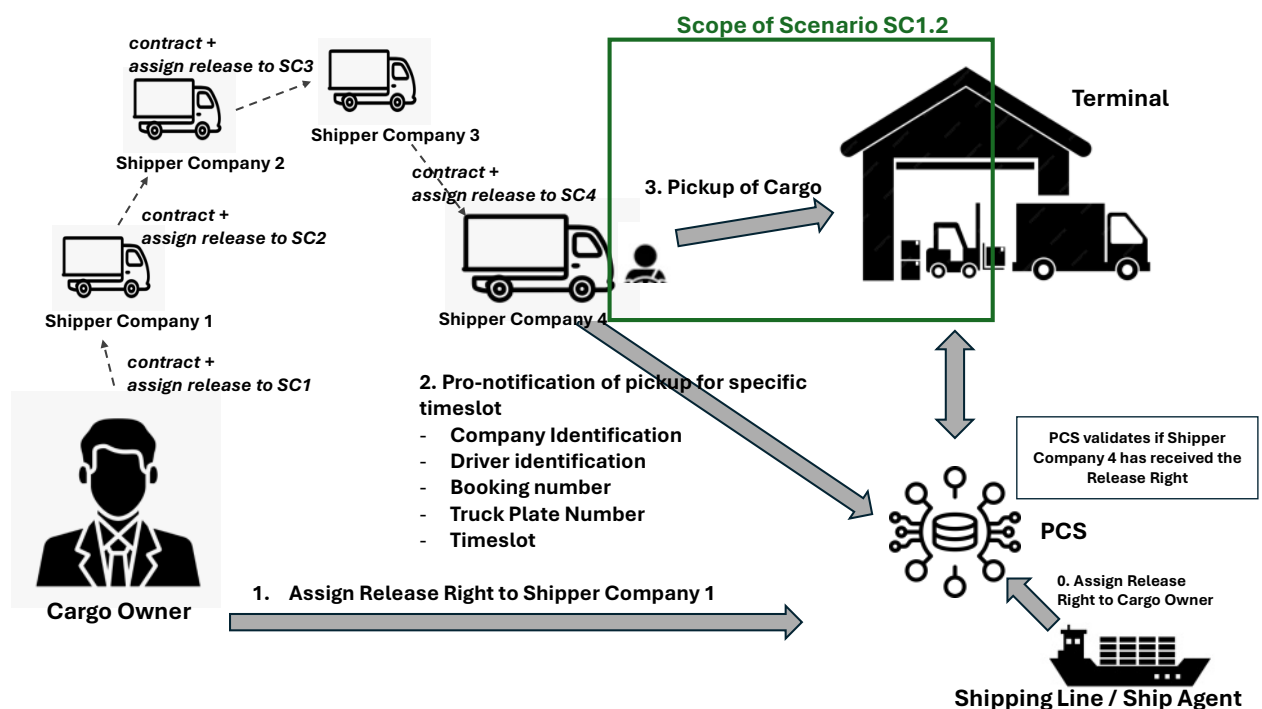
1.2 Scenario introduction

This scenario purpose is to authorise pickup/delivery of cargo by Identifying with the wallet, carrier, driver and truck for transparent and safe operation:

- Identify and authenticate carrier, driver and truck for secure gate access to port territory and transparent operations.
- Enable delivery acceptance transactions within Terminal Operating System (TOS) using wallet-verified credentials and authorisation for access to port infrastructure and restricted areas.

The scenario will work with existing PCS implementations but will not undertake comprehensive PCS (Port Community System) redesign or replacement.

The scenario assumes the availability of compliant Wallet from participating Member States; it does not develop wallet infrastructure itself even if any developments on wallets and infrastructure needed for piloting will be addressed in WP4.



The scope of the scenario is to identify the driver and its company at the time of accessing the terminal for picking up the cargo. Many other checks (and scoring) are done at the very same time; they are out of the scope of the scenario (examples):

- Transport permit
- Driver license
- Safety instructions
- Dangerous goods certificate (BU5)
- Information received in prenotification

The use case focuses on road transport and maritime/inland port operations; the inclusion of rail transport and inland waterways are also out of scope.

The pilot focuses on EU cross-border scenarios only; non-EU jurisdictions are not included.

The scenario is based on the following documentation:

- Stocktaking document

2 Scenario specification

2.1 Introduction

SC1.2 is an MVP scenario.

A driver which is an employee of a company A (country A) wants to access to a terminal B located in country B. Thus, a mobile Wallet is a must have as well as proximity flow with offline capability (the gates at the terminal that allow physical access must not be dependable on infrastructures). The driver belongs to the same organisation than the company. The driver is using a mobile device.

The terminal (relying party) needs of validate the company: different ports use different methods. Some identify the person, others the business and both approaches should be supported for interoperability reasons. The goal is to make both identifications to improve security (cargo theft).

The following credential will be processed

- EBWID from company A
- POX attestation as “employee attestation” -> POE

More attestations identified in the stocktaking document are no longer needed:

- EUCC: That attestation brings information about the company of the driver. That information is not needed to allow access. Only identification is required.
- Powers of Representation/Authorisation attestation information is included in the POE attestation
- Cargo Token, Terminal Access authorisation and Holder specific authorisation are now out of the scope as there are included in the pre-notification process. Only identification information is needed.

To identify a particular employee (natural person) without a PID, an employee identifier “professional id” is introduced and will be included in the employee attestation. A revocation must be done when employee leaves the company (not in real time but within a short delay)

Other specific needs

- One (and only one) wallet app. on device for the employee (the driver)
- The driver may not be able to access a BW

Natural person wallet (NW) cannot be compulsory. We should not enforce employees to use their personal wallet (NW) for business interactions.

Therefore, the wallet used in this scenario is a wallet that could be a mobile or a stripped-down version of a BW. That wallet holds credentials relevant to the employee, while the business wallet has broader issuing and verification capabilities.

The expected wallet behaviour is:

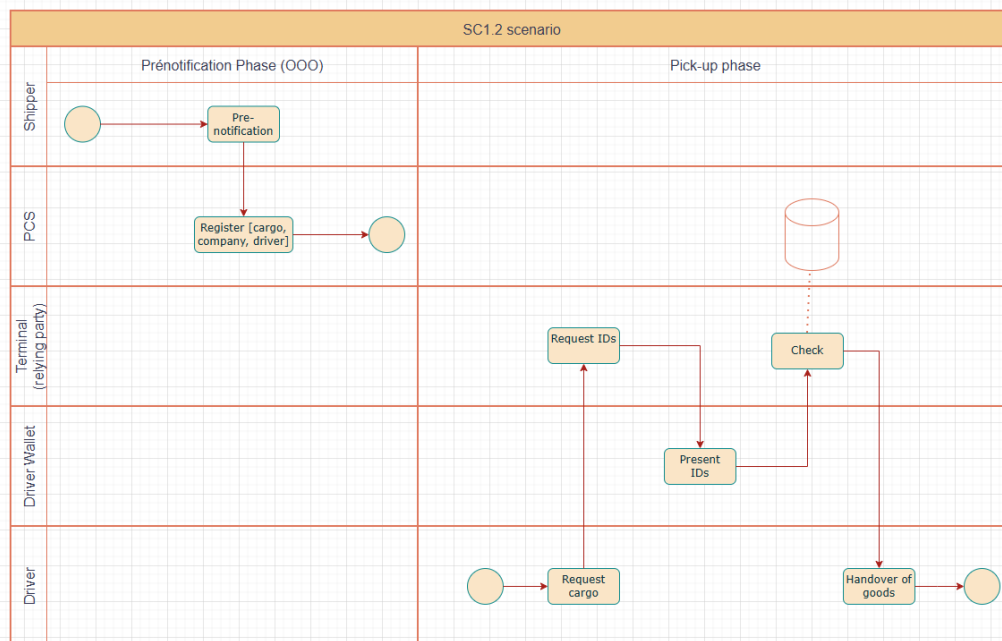
- The wallet is issued and managed by the Employer.

- It's not living in the cloud but downloaded on a mobile phone of the employee. That mobile phone is only used by that employee. [biometric authentication (e.g., face or fingerprint recognition) to ensure strong binding to the individual driver.
- Employer must revoke employee wallet when employee leaves the company
- No need of a certified Wallet (PID & LOA high not needed)
- Contain a professional ID which is not a qualified attestation, but an EAA issued by employer
- The wallet is personal and non-transferable

2.2 Scenario pre-conditions

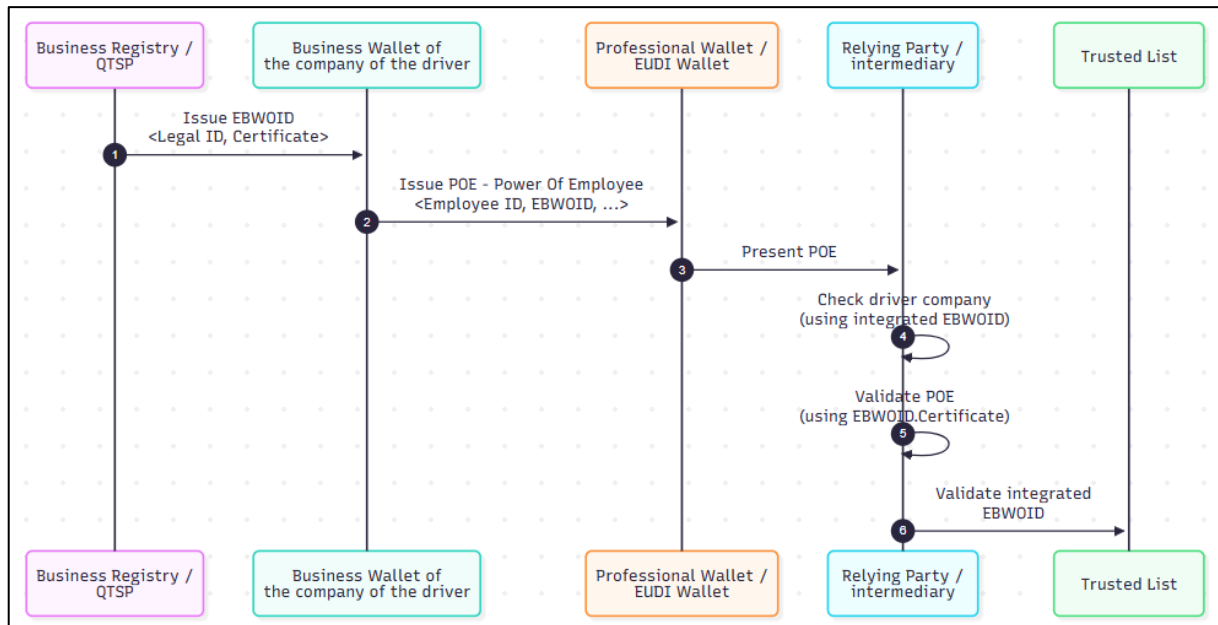
The availability of a valid is a prerequisite. A Wallet, it is installed, operational and has an issued EBWOID. The carrier company needs to have a valid BW capable of issuing an EAA attestation.

2.3 Scenario main flow



The prénofication phase (left column) is out of the scope of the scenario.

Basically, the driver needs to have a wallet with EBWOID and POE.



2.4 Scenario alternate flow

Intended variations to be piloted and investigated in testing/piloting.

Flow	Short description
- Wallet variations	Depending on the availability of wallets, EUDI wallet of the driver as a natural person
- POE usage	Check by the relying party of the company or the driver identification or both depending on its policy
- Sole trader	The same wallet could be used for multiple clients if the driver is a sole trader

Optionally, at the exit of the terminal, the driver could be checked at the gate. That event could initiate the handover of the goods with an eCMR (see scenario SC1.3).

2.5 Challenges and barriers (fast and secured)

ID	Level	Challenge
1	Low	The employer/ee attestation has no existing rulebook, SC1.2 scenario needs should fit into the POX/POE attestation, but it has to be checked carefully (or POE model updated).
2	Medium	Credentials revocation. Revocation mechanisms may be not optimised for that gate access/checkpoint scenario where close to real-time status checking is needed. A balance between security and usability must be found i.e. short-lived, status list, revocation list mechanisms.
3	High	Fast access to terminal is a key factor. The proximity flow must be check in detail: simplicity to use from the driver point of view, offline capabilities, security linked with the device (device-based biometric verification such as facial recognition or fingerprint checks)
4	Medium	Sole traders case compliancy with the scenario.

2.6 Working Assumptions

A wallet as defined in scenario pre-conditions is expected.

The scenario assumes that the business registers can issue an EBWOID or that QTSP will do it if business registers are not available for the countries expected.

Onboarding information / IDs needed and cargo related needed are known from the RP.

The scenario assumes that only test data and a pre-production environment will be use.

3 Detailed scenario flow

As a pre-requisite, it is expected that the employee (the driver) has a device (provided or not by its enterprise). On that device, the wallet of the driver has been setup and is only accessible to present attestations by that very same driver.

Per step in the main flow, a detailed description is made in the table below.

Flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
1. Issue EBWOID	Business Registry / QTSP & Business Wallet of the company of the driver.	The BW of the company of the driver receives its own EBWOID and store it	Trusted issuers registered in a Trusted List.	Could be considered as a pre-requisite
2. Issue POE	Business Wallet of the company of the driver. & Proximity Wallet / EUDI Wallet	The driver initiates a request through its wallet to obtain the attestations needed: POE and the EBWOID of his company.		
		The BW of the company issues the POE requested		
		The driver's wallet stores the received attestations		
3. Present POE	Proximity Wallet / EUDI Wallet & Relying Party (RP) / intermediary	The RP defines the required attribute and builds the presentation request		
		The driver receives the request (QR code?) and accepts it with his wallet to share the attestations requested		
		The RP receives the information		
4. Check driver company	Relying Party / intermediary	The RP checks the driver's company by using integrated EBWOID		
5. Validate POE	Relying Party / intermediary	The RP validates the driver's POE integrity by using EBWOID Certificate		
6. Validate integrated EBWOID	Relying Party / intermediary & Trusted List	RP verifies the presentation and trust chain via the WeBuild Trusted List		

Then, the RP is doing other checks to allow access to the terminal for picking up the cargo. The OK/NOT OK information back to the driver (outcome) is not done with Wallet.

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of Wallet	Companies on behalf of relying parties, see 4.3	BE, DE, ES, FR, NL, PL
2. Authentic sources	EBWOID issued by WP4 and/or other UC. Those partners are not in SC1.	
	if there is no business register to act as authentic source, WP4 will create one to cover EBWOID issuing for pilot purposes	BE
		DE
	Registadores	ES
	Infogreffe	FR
	KvK	NL
	MRIT	PL
3. Intermediary+Relying party	SC1 Partners act as intermediary and will involve a port authority (terminal) which could not be a WeBuild Partner	
	Secure Logistics + Rotterdam Shortsea Terminals	NL
	Portic + [Port authority/terminal collaboration]	ES

4.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. Wallet provider	Digidentity Credinco Sphereon (tbc)	NL NL DE	BW BW
2. PID Provider			
3. Trusted list registrar			
4. QEAA provider	To be identified with WP4		
5. Pub-EAA provider			
6. EAA provider	Chosen companies, see 4.3		
7. QES provider			

4.3 Target country combinations

Due to geographic and operational factors, the choice of holders (companies and drivers) will target countries near the relying parties (terminals) and will be made when concrete things are available to be shown. The terminals have several thousands of customers and will allow to find holders (companies and drivers)

The scenario has 2 relying parties. Cross border combinations can easily made by choosing a company in a different country than the relying party.

	Issuing country						
Relying Party country		BE	DE	ES	FR	NL	PL
	ES				X		
	NL	X	X		X		X

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex.

5 Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners) or are to be provided by other use cases or working groups.

This section clarifies which attestations will be of what type, while the details of each attestation that will be created within the scenario itself, will be described in detail in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenarios

Attestation name	Short description	To be provided by	For Countries	Requirements
EBWOID	European Business wallet owner identification	WP4 PID LPID group	BE, DE, ES, FR, NL, PL	
POX/POE	Employer/employee attestation	BU4	BE, DE, ES, FR, NL, PL	Issued by companies with their business wallet
PID	PID	WP4 PID LPID group	BE, DE, ES, FR, NL, PL	For variation where an EUDIW is used as providing a PID cannot be mandatory for an employee

5.3 Created attestations in the scenario

No attestation should be created for this scenario. The employer/employee attestation needs should be embedded in the POE attestation designed by BU4. The POE attestation gives details of the employee/driver and proves that the employee is still belonging to its company. The relying party can check the employee details and the company Id.

Nonetheless, specifics requirements are still to be checked with that design:

- Company Identity proofing / matching with BW still looks to be an issue to solve, either with an Id of the company (from the business wallet) or the full business wallet credential.
- Employee number or professional id exists
- Non-qualified attestation EAA is possible
- Proximity flow compliancy (i.e. mdoc format)
- The attestation in the wallet can be cryptographically bound to the wallet, ensuring that only the intended employee can use it, and that the attestation is verifiable as being issued by the business wallet of the company

If those requirements are not fulfilled, then a fork of that design could be created.

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario.

Primary role	Specific requirement
1. User of Wallet	a.
	b.
	c.
2. Authentic sources	a. Business registers will issue an EBWOID
	b.
	c.
3. Relying party	a. Has a functioning gate access platform
4. Intermediary	b. Able to accept EBWOID and POE attestations
	c.
5. Wallet provider	a. will provide a personal wallet to the employee/driver of a company
	b. will provide a business wallet that includes the EBWOID of that company
	c. will provide a proximity interface on mobile devices to the personal wallet.
	d. will ensure a strong binding between the mobile device used and the individual employee/driver user of the personal wallet
	e. will be capable to issue a PoE EAA attestation to the personal wallet used by the employee/driver on behalf of the company of the employee/driver (business wallet -> personal wallet)
	f. will authorize the company to revoke that attestation
	g. will support mdoc format for that attestation
	h. will make the wallet usable offline
	i. will prevent another person to use the personal wallet. The wallet is personal and non-transferable.
	Note: no need of a certified Wallet (PID & LOA high not needed)
6. PID Provider	a.
	b.
	c.
7. Trusted list registrar	a.
	b.
	c.
8. QEAA provider	a.
	b.
	c.
9. Pub-EAA provider	a.
	b.
	c.
10. EAA provider	a.
	b.

	c.
11. QES provider	a.
	b.
	c.

Specification Scenario 1

<Seamless onboarding>

WP2 – SC2 Trusted Data Sharing for Data Spaces

Date : 19/06/2026

Version : 1.0 (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)

Status : Final (Draft, for review, reviewed, final)

Table of contents

Table of contents	2
1. Introduction.....	4
1.1 Objectives of this document	4
1.2 Scenario introduction	4
2. Scenario specification.....	5
2.1 Introduction.....	5
2.2 Scenario pre-conditions	6
2.2.1 Identity and participant readiness	6
2.2.2 Availability of required attestations	6
2.2.3 Wallet availability and readiness.....	7
2.2.4 Standards and interoperability	7
2.2.5 DSI technical capabilities	8
2.2.6 Data space governance and trust alignment	8
2.3 Scenario main flow.....	9
2.4 Scenario additional flows	12
2.5 Challenges and barriers.....	13
2.5.1 Technical challenges	13
2.5.2 Legal challenges	14
2.5.3 Organisational challenges	14
2.5.4 Standardization challenges	15
2.6 Working Assumptions.....	15
2.6.1 Wallet availability and functionality.....	15
2.6.2 Credential issuance and usage	15
2.6.3 Acceptance of wallet-based onboarding	16
2.6.4 Governance alignment	16
2.6.5 User adoption.....	16
2.6.6 Standards maturity	16
2.6.7 Trust infrastructure	16

3.	Detailed scenario flow.....	16
3.1	Scenario 1 – User story 1.....	17
3.2	Scenario 1 – User story 2.....	20
3.3	Scenario 1 – User story 3.....	22
4.	Roles and participants.....	24
4.1	Scenario roles and participants.....	24
4.2	Additional roles and partners	25
4.3	Target country combinations	26
4.4	Requirements	26
5.	Attestations.....	26
5.1	Introduction.....	26
5.2	Attestations to be provided by other UCs/WGs/scenario.....	26
5.3	Created attestations in the scenario.....	27
	Annex 1 – Requirements for scenario roles	28

1. Introduction

1.1 Objectives of this document

The document focuses on Scenario 1: **Seamless onboarding across Data Space Initiatives** (DSIs), which forms the core MVP of the use case of the Supply Chain 2 (SC2) within Work Package 2 of the WE BUILD consortium.

It provides a detailed specification of:

- Scenario 1 onboarding processes that are aimed to be piloted within a mini dataspace, for this pilot called: “Agri-X”¹
- The attestations and credentials to be issued, presented, and verified within this scenario 1
- The roles and responsibilities of participating partners

This specification is aligned with:

- The Stocktaking document
- The **updated** Attestation Description document: Membership credential
- The overall WE BUILD architecture and WP4 guidance

This document is the result of the Specification Phase of the WE BUILD Large Scale Pilot and represents an important step towards the implementation and validation of the use case needed for piloting.

The learnings from this scenario are expected to support future MVP+ scenarios and broader adoption of interoperable onboarding mechanisms within European Data Spaces.

1.2 Scenario introduction

- **More detailed:** The scenario addresses cross-border onboarding of Legal Persons/Organizations across Data Space Initiatives(DSI) using EUDI Wallet-based verifiable credentials(Membership credential), validated within a controlled mini dataspace environment(“Agri-X”).

¹ Although the ambition of the piloted scenario is to draw lessons-learned and share or apply these in the CEADS project, we will use the term “Agri-X” to make a clear distinction that these are separate projects and evolve at their own pace.

- **Less detailed:** Cross-border onboarding of organisations in dataspace like CEADS, Catena-X, ... using EUDI Wallet-based membership attestations.

The scenario is based on the following documentation:

- [ARF version](#)
- [Stock Taking document](#)
- [WP4 Architecture and Integration Blueprint D4.1](#)
- [Sole trader discussion](#) from WP4

2. Scenario specification

2.1 Introduction

This MVP scenario focuses on seamless onboarding of Legal Persons across multiple Data Sharing Initiatives (DSIs) using EUDI Wallet-based verifiable credentials.

The scenario is implemented within a ‘mini’ dataspace environment, within this pilot referred to as “Agri-X”, that consists of three DSIs - DjustConnect, DIH Agrifood Data Space (DADS) and Tritom - and serves as a pilot towards broader Data Space adoption (e.g. CEADS, SAGE, Catena-X, etc).

The scope of this MVP scenario is the issuance of a membership credential that can show users of the EUDI business wallet with which data platform an organization is sharing data with or consuming data from.

This credential is a business-level attestation and is not related to any technology used for the actual data transfer, nor the credentials used within these technologies which are considered out of scope.

In this scenario, a Legal Person (including one-person companies acting as legal entities):

- Onboards at one DSI A by accepting the governance rulebook of the DSI
- (*) Additionally may accept the governance rulebook of the dataspace “Agri-X”
- Receives:
 - a Membership credential specific to the DSI
 - (*) a Membership Credential for the ‘mini’ dataspace
(Both credentials use the same credential schema)
- Stores these credentials in a digital wallet

These credentials can then be presented to another DSI (DSI B), which can verify them and allow onboarding without requiring full re-registration in case governance rulebooks are compliant or accepted before.

The three participating DSIs will be the issuer of membership credentials for their specific DSI, while they are also an onboarding service provider for the ‘mini’-dataspace “Agri-X”.

Note: The seamless onboarding scenario will also be explored as an MVP+ scenario where an additional (dataspace) trust layer is added via a (dataspace) Trust Framework. This MVP+ scenario will use different attestations (see deliverables for the MVP+ scenario itself).

Note: This scenario focuses on Legal Person (LP) onboarding. Natural Person (NP) wallets and representation mechanisms are out of scope for this MVP. More advanced features, such as mandates and delegation, are out of scope for this MVP, but will be explored in subsequent scenarios (MVP+).

2.2 Scenario pre-conditions

The execution of this scenario depends on a set of technical and organizational preconditions, ensuring that onboarding and credential exchange can be performed in a secure and interoperable manner across the participating Data Sharing Initiatives (DSIs).

2.2.1 Identity and participant readiness

- Both the end-user and the DSIs have a EBW available that uses the same credential format
- Legal Persons (including one-person companies like farmers acting as legal entities) must be identifiable using authoritative identifiers, such as:
 - EBW-OID
 - VAT number via VAT-ID credential

Note: Both attestations will be mocked.
- The MVP does not rely on the European Company Certificate (EUCC), but remains compatible with future adoption of EUCC-based credentials.

2.2.2 Availability of required attestations

The following attestations must be available and usable within the scenario:

- EBW-OID
- VAT ID

- Dataspace Membership Credential (issued during onboarding within this scenario)

Important remark: JSON-LD is the primary format for semantic interoperability in this scenario, SD-JWT may be explored in parallel or in a later phase for interoperability testing. The reasons for using JSON-LD are explained in the Chapter 2.3 Scenario Main Flow.

In case a business wallet only supports a single format, this requires also the EBW-OID and VAT-ID to be issued as JSON-LD.

Another option is that the business wallet supports both formats and implements OpenID4 VCI 1.1 together with the interactive authorization endpoint which would allow the onboarding partner to hold the EBW-OID and VAT ID attestation issued by the authentic sources as SD-JWT, present it and receiving the DS Membership credential issued by the DSIs as JSON-LD.

Note: The KMG-MID issued by the Ministry of Agriculture in Slovenia and used by the DADS platform is kept out of scope for this pilot.

Note: As none of the Business Registries related to the member states of the 3 DSIs are represented in the UC, the prerequisite attestations will be mocked.

2.2.3 Wallet availability and readiness

Participants must have access to a business wallet that is:

- Installed and operational
- Capable of storing and presenting Verifiable Credentials (VCs) and Verifiable Presentations (VPs)
- Supporting the W3C Verifiable Credential Data Model (VCDM) together with the JSON-LD format

The wallet must be capable of handling:

- Dataspace Membership Credential (UC specific attestation)
- Supporting identity attestations (e.g. EBW-OID, VAT-ID)

Given the current maturity of the ecosystem and the support for JSON-LD, the scenario may rely on:

- Pre-EUDI or intermediate wallet solutions
- Wallets integrated with DSI platforms

2.2.4 Standards and interoperability

All credential-related interactions must be based on:

- W3C Verifiable Credentials (VC)

- Verifiable Presentations (VP)

The use of W3C VCDM is required to:

- Ensure interoperability across DSIs
- Enable future extension to additional attestations (e.g. data usage licenses, DPP-related credentials)

2.2.5 DSI technical capabilities

Participating DSIs must support (either directly or via a technology solution):

- Issuance of verifiable credentials (Dataspace Membership Credential)
- Verification of credentials presented by participants
- Integration with wallet solutions
- Basic interoperability with:
 - Identity providers

2.2.6 Data space governance and trust alignment

- The participating Data Sharing Initiatives (DSIs) that are involved in this pilot must operate within an established and operational data space environment, where:
 - Common rulebooks and onboarding requirements are defined
 - Participants are onboarded under agreed governance conditions (by presenting their local (economic) identifiers and accepting the dataspace governance rulebook)
- The DSIs participating in the scenario (mini dataspace) must have:
 - Established mutual trust relationships
 - Alignment on
 - Onboarding procedures
 - Credential usage
 - Verification rules
 - Be recognised as issuer and relying party within the EUDI Framework Trust Infrastructure for EAA (LotE, credentials catalogue)
- This includes:
 - Agreement on a common or aligned rulebook for the mini dataspace (defining the rulebook itself is out of scope for this project)
 - Recognition of each other's onboarding processes and issued credentials

This prerequisite ensures that:

- Credentials issued by one DSI can be trusted and accepted by another

- Cross-platform onboarding is possible without repeating full registration

2.3 Scenario main flow

The seamless onboarding will consist of 2 main user stories where:

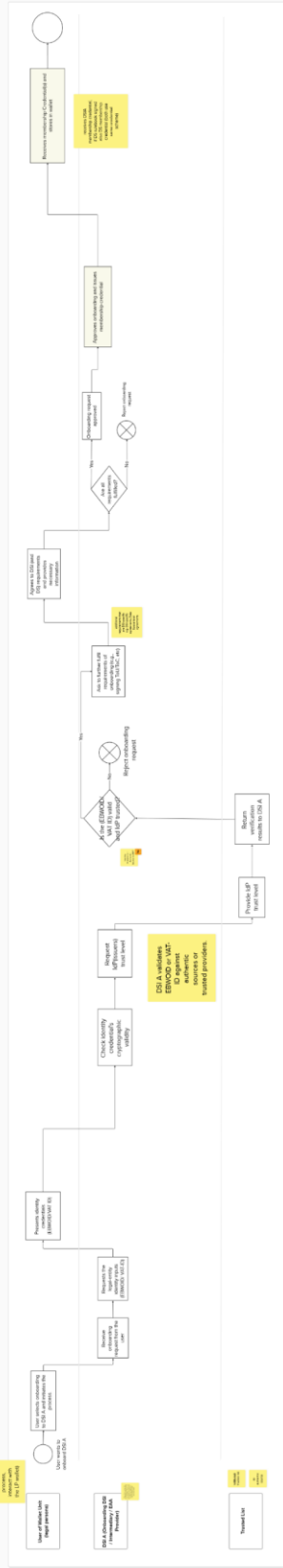
- 1) The end-user onboards with a (local) DSI and potentially with the EU mini-dataspace “Agri-X” which results in single or multiple membership credentials.
- 2) The issued membership credentials are then presented (cross-member state and cross-DSI) to onboard into another DSI

Because of the importance of the JSON-LD format within the dataspace domain and its semantic interoperability the preference in our Use Case would be to pilot this format. However as the main focus of most wallet providers is SD-JWT as well as there is no guarantee that business registries will eventually issue VAT-ID in the JSON-LD format we consider piloting both credential formats in a phased approach. (See additional flows)

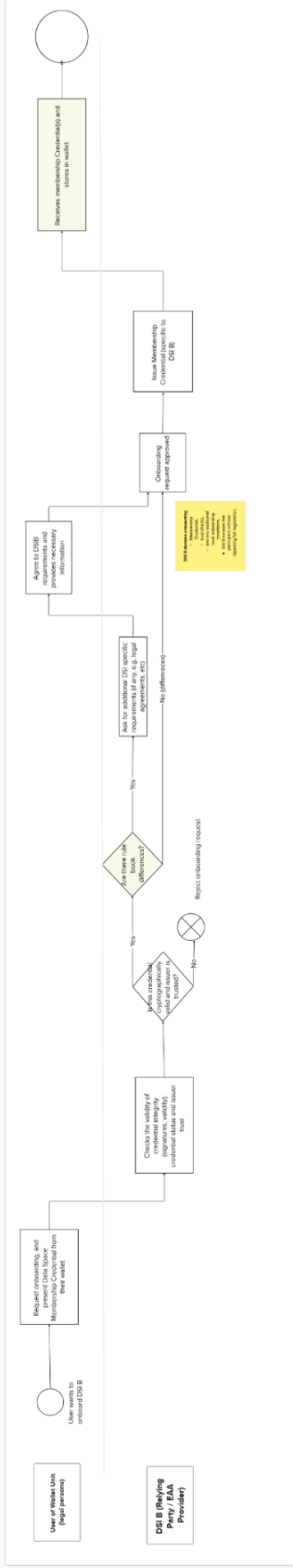
Next to onboarding new members based on a wallet, we consider also to pilot a third user story focusing on issuing the membership credential to existing members of a DSI. For this user story the main difference is that the user story is triggered by the end-user from within the DSI portal.

Inbound flows

User story 1 - MVP scenario: first onboarding to DSI A

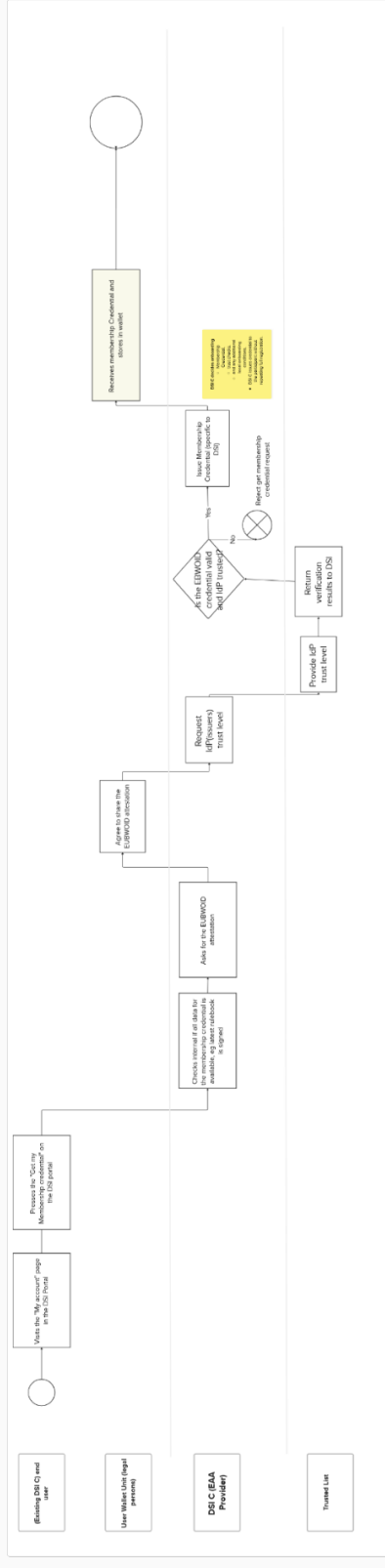


User story 2 - MVP scenario: reuse credential to onboard second DSI B



Outbound flow

User story 3 - MVP scenario: issue credential to previously onboarded DSI members



Since the flow is extensive, better to look at the **Mural** directly:

<https://app.mural.co/t/ilvo1917/m/xuelinilvo3024/1770371652460/c44884eac8599d3b6c36f6dca45bc9ac8c55a54b>

2.4 Scenario additional flows

In addition to the main onboarding flow, the scenario includes a limited number of variations and exceptions that are considered relevant for piloting. Only variations and exceptions that are expected to be tested during the pilot are included in this section.

Technical exceptions and implementation-specific error handling (e.g. network failures, wallet software issues, or protocol-level errors) are considered out of scope for the scenario specification and will be addressed during implementation and testing activities where relevant.

Flow	Short description
Variations	
Standard onboarding (main flow)	Onboarding flow with JSON-LD as credential format
Standard onboarding (main flow)	Onboarding flow with SD-JWT as credential format
Existing members flow	User story 3: Instead of starting the issuance of the membership credential via the wallet, a DSI can use a shorter flow for existing members
Exceptions	
Invalid credential	If the presented identity credential (e.g. EUDI, PID, EBWOID, VAT) is invalid or cannot be verified, the onboarding request is rejected
Untrusted issuer	If the identity provider or credential issuer is not trusted (based on trust lists/registries), onboarding is rejected
Incomplete requirements	If the user does not fulfill additional onboarding requirements (e.g. does not accept the rulebook), the onboarding request is rejected

The following aspects are not part of this MVP scenario but are expected to be addressed in future scenarios (MVP+):

1. Mandates and representation of natural persons within the legal entity/ on behalf of the legal persons
2. Delegation of rights and access across organizations
3. Use of data usage licenses

2.5 Challenges and barriers

The development and piloting of Scenario 1 involves several technical, organizational, and standardization challenges. These are influenced by the evolving nature of the EUDI Wallet ecosystem and the need to align multiple actors within a cross-platform data space environment.

2.5.1 Technical challenges

- Maturity of the EUDI Wallet ecosystem
 - The EUDI Wallet ecosystem is still evolving and not yet fully harmonized across Member States. As a result, the pilot must rely on pre-EUDI or intermediate wallet solutions, which may differ in capabilities and interfaces.
- Interoperability of identity attributes and credentials
 - The scenario relies on multiple identity attributes and identifiers (e.g. EBW-OID, VAT) that are incorporated into credentials such as the Dataspace Membership credential. Differences in formats (JSON-LD vs SD-JWT), schemas, and issuance mechanisms may lead to interoperability challenges across DSIs and wallet providers.
- Credential verification and trust infrastructure
 - Verification of credentials requires:
 - Validation of issuer trust (via trusted lists or registries) for which the provided trust infrastructure might only be fit4pilot
 - Checking credential integrity and status
- Integration with existing DSI platforms
 - Existing data sharing platforms (DSIs) are not natively designed for wallet-based onboarding. Integration of:
 - VC/VP exchange
 - Credential issuance and verification.

2.5.2 Legal challenges

- Cross-border regulatory differences
 - Variations in national regulations related to:
 - Legal representation
 - Consent
 - Liabilitymay impact the consistency of onboarding processes across DSIs.
- Legal status of wallet-based credentials
 - The legal recognition of wallet-based credentials, particularly **non-qualified attestations (EAAs)** used in this MVP, is still evolving. Their acceptance depends on:
 - Contractual agreements and/or rulebooks
 - Credential catalogue with the necessary LotE attached
- Data protection and GDPR compliance
 - The handling of identity data and credentials must comply with GDPR, including:
 - Minimisation of data sharing
 - Secure storage and transmission
 - Clear allocation of responsibilities between actors

2.5.3 Organisational challenges

- Adoption by smaller actors

Target users such as farmers and SMEs may face barriers related to:

 - Limited digital maturity
 - Complexity of wallet usage
 - Lack of familiarity with credential-based onboarding
- Coordination across multiple stakeholders

The scenario requires alignment between:

 - DSIs (acting as issuers, verifiers, and intermediaries)
 - Wallet providers
 - Identity providers (not represented for the 3 member states of the DSIs)
- Ensuring consistent implementation across these actors is organizationally complex.
- Alignment of rulebooks and governance

Differences in rulebooks and onboarding requirements between DSIs may hinder seamless onboarding. Deciding a common governance rulebook for the mini dataspace is out of scope of this pilot. For the dataspace governance level a preliminary rulebook will be used to pilot the scenario.

2.5.4 Standardization challenges

- Evolving standards for wallets and credentials
Standards such as:
 - W3C Verifiable Credentials
 - EUDI Wallet specifications
 - OpenID4VC protocolsare still evolving, which may lead to:
 - Changing requirements
 - Compatibility issues
- Interoperability challenge due to different credential formats (JSON-LD vs SD-JWT). It is unclear if all attestations we depend on will be delivered in both formats.
- Dependency on external components
The scenario depends on external elements that may not yet be fully mature or available, including:
 - Identity providers (EBW-OID)
 - Wallet implementations
 - Trust List registries and infrastructure
- This creates uncertainty in implementation timelines and integration effort.

2.6 Working Assumptions

Due to the evolving nature of the EUDI Wallet ecosystem and related standards, the following working assumptions are defined to support the development and piloting of Scenario 1.

2.6.1 Wallet availability and functionality

- A business wallet (EUDI Wallet or equivalent) is available and usable in the pilot
- The wallet supports storage and presentation of Verifiable Credentials (VCs) and Verifiable Presentations (VPs) compliant with W3C VCDM
- The wallet supports the credential format that is part of the flow

2.6.2 Credential issuance and usage

- Verifiable Credentials can be issued, stored, and presented across DSIs
- The following credential schema is available in a credential catalogue
 - Dataspace Membership Credential (issued by DSIs)
- Identity attributes (e.g. EBW-OID, VAT-ID) are available for verification and inclusion in credentials. These will be mocked attestations as none of the member state authentic sources is part of Webuild for the three DSIs

2.6.3 Acceptance of wallet-based onboarding

- DSIs accept wallet-based credentials for onboarding
- DSIs recognize credentials issued by other DSIs within the mini dataspace

2.6.4 Governance alignment

- Participating DSIs have defined a (mock) common rulebook for the Agri-X dataspace level and the rules on how to act when difference exist between the rulebooks

2.6.5 User adoption

- Participants (Legal Persons) are able and willing to use a business wallet for onboarding or storing a membership credential

2.6.6 Standards maturity

- Relevant standards (e.g. **W3C VC**, **EUDI Wallet specifications**) are sufficiently stable for pilot implementation

2.6.7 Trust infrastructure

- The UC MVP scenario will pilot directly on the trust infrastructure provided by Webuild using the Credential Catalogue² and the related LoTL/LotE provided by the Trust group in WP4 to be able to verify the trusted issuers for the credentials used.
- The prerequisite Identity attestations like EBW-OID and VAT will be present in the Credential Catalogue and WP4 participants providing the mock attestations will be included in the relevant LotE.

The use case is only responsible for adding the UC specific information related to the Dataspace Membership credential

3. Detailed scenario flow

Per step in the user stories, a detailed description is made in the table below.

It is important to note that within Scenario 1, there are 3 user stories that are divided into 3 swimming lane diagrams as well. There is User story 1 of the scenario, when the User of the Wallet Unit requests onboarding first to DSI A (Onboarding DSI / Intermediary / EAA Provider). In the second user story the user will reuse a previously issued membership credential to onboard in a second DSI.

² Credential catalogue might be optional for EAA

Finally there is a user story that will pilot the outbound flow for issuing the membership credential. This means that the issuance of the membership credential will be triggered from within the DSI platform for members that onboarded via a non-wallet way. This allows for adoption of the membership credential by existing members of the DSIs.

3.1 Scenario 1 – User story 1

First onboarding to DSI A

Actor	Interpretation or reference	Dependencies	Variations and exceptions
STEP 1 – Initiate Onboarding			
User of Wallet Unit (legal persons)	User selects onboarding to DSI A and initiates the process in the DSI interface	Wallet available and operational (EBW-OID and VATID available in the wallet)	User of Wallet unit or the authorised representative can start the process.
DSI A (Onboarding DSI / Intermediary / EAA Provider)*	Receives onboarding request and initiates the identification process	DSI onboarding interface available	The onboarding request may be automatically rejected/labelled as unsuccessful if the DSI onboarding platform is unavailable
<i>*The parts that are in bold indicate the role that the actor plays in this step, since this actor can play multiple roles across the scenario based on the ARF role definitions.</i>			
STEP 2 – Request for and presentation of identity credentials			
DSI A (Onboarding DSI / Intermediary / EAA Provider)	Requests identity credentials (EBWOID + 1 local identifier like VAT-ID) from the user	Wallet + credential support	Additional attributes may be requested depending on DSI
User of Wallet Unit (legal persons)	Presents identity credentials from the wallet	Availability of identity credentials	If attributes missing → onboarding cannot proceed
STEP 3 – Identity verification by DSI as Relying Party			
(Note: One or more of the following steps can be outsourced by DSI to technology providers)			
DSI A (Onboarding DSI / Intermediary / EAA Provider)	Verifies credential integrity and content (signature, validity)	VC standards (e.g. W3C VC)	Invalid credential → rejection

DSI A (Onboarding DSI / Intermediary / EAA Provider)	Verifies the issuer and credential status	Status list and Trusted list	—
STEP 4 – Decision on identity and trust by DSI as Relying Party			
DSI A (Onboarding DSI / Intermediary / EAA Provider)	Evaluates whether the identity credential (EBWID/VAT) is valid and the issuer is trusted	Successful verification	If not valid → onboarding rejected
DSI A (Onboarding DSI / Intermediary / EAA Provider)	If valid, proceeds with further onboarding requirements	Identity verified	—
STEP 5 – Onboarding requirements			
DSI A (Onboarding DSI / Intermediary / EAA Provider)	Requests to fulfill onboarding requirements (Requirements that are Data Space specific + additional requirements that are DSI platform specific e.g. Data Space level agreements, DSI specific agreements)	Requirements defined and accessible	Requirements may differ per DSI
User with the wallet (legal persons)	Provides any required information and agrees to DSI or DS specific requirements (no QES for this pilot)	User interaction	If not fulfilled → onboarding rejected
DSI A (Onboarding DSI / Intermediary / EAA Provider)	Evaluates completion of requirements	Completion of onboarding inputs	Missing data → request additional input
STEP 6 – Final decision on Onboarding			
DSI A (Onboarding DSI / Intermediary / EAA Provider)	Confirms that all onboarding conditions are met	Identity + requirements validated	If not fulfilled → rejection

STEP 7 – Membership Credential Issuance by DSI as EAA provider			
DSI A (Onboarding DSI / Intermediary / EAA Provider/ Issuer)	Issues Membership Credential	VC issuance capability	—
DSI A (Onboarding DSI / Intermediary / EAA Provider/ Issuer)	Sends Membership Credential(s) to wallet	Wallet capable of receiving credentials	Delivery failure → retry
STEP 8 – Storage in wallet			
User /Wallet	Receives and Stores Membership Credential	Wallet storage capability	Storage failure → retry or error

3.2 Scenario 1 – User story 2

Second onboarding to DSI B

Actor	Interpretation or reference	Dependencies	Variations and exceptions
STEP 1 – Initiate Onboarding in DSI B			
User of Wallet Unit (legal persons)	User selects onboarding to DSI B and initiates the process in the DSI interface	Wallet available and operational membership credential DSI A available	User may access onboarding via wallet-native flow instead of DSI UI
DSI B (Onboarding DSI / Intermediary / EAA Provider)*	Receives onboarding request and initiates the identification process	DSI onboarding interface available	The onboarding request may be automatically rejected/labelled as unsuccessful if the DSI onboarding platform is unavailable
<i>*The parts that are in bold indicate the role that the actor plays in this step, since this actor can play multiple roles across the scenario based on the ARF role definitions.</i>			
STEP 2 – Request and presentation of credentials			
DSI B (Onboarding DSI / Intermediary / EAA Provider)	Requests credentials from the user	Wallet + credential support	Additional attributes may be requested depending on DSI
User of Wallet Unit (legal persons)	Presents EBWOID/VAT and Membership Credential from wallet	Credentials stored in wallet	Missing credentials → onboarding cannot proceed
STEP 3 – Credential verification by DSI B as Relying Party			
DSI B (Onboarding DSI / Intermediary / EAA Provider)	Verifies credential integrity and content (signature, validity)	VC/VP verification capability	Invalid credentials → onboarding rejected
DSI A (Onboarding DSI / Intermediary / EAA Provider)	Verifies the issuer and credential status	Status list and Trusted list from PR	
STEP 4 – Decides if there are governance differences			

DSI B (Onboarding DSI / Intermediary / EAA Provider)	Evaluates if presented membership credentials are enough by comparing rulebook differences		If not valid → onboarding rejected
DSI B (Onboarding DSI / Intermediary / EAA Provider)	If differences, proceeds with additional onboarding requirements, if no differences to final decision on onboarding	DSI-specific policy if any	Some DSIs may require additional checks
STEP 5 – Additional onboarding requirements			
DSI B (Onboarding DSI / Intermediary / EAA Provider)	Requests to complete additional onboarding requirements that are DSI platform-specific	Requirements defined and accessible	Requirements may differ per DSI
User with the wallet (legal persons)	Provides required information and accepts conditions (no QES in this pilot)	User interaction	If not fulfilled → onboarding rejected
DSI B (Onboarding DSI / Intermediary / EAA Provider)	Evaluates completion of requirements	Completion of onboarding inputs	
STEP 6 – Final decision on Onboarding			
DSI B (Onboarding DSI / Intermediary / EAA Provider)	Confirms that all onboarding conditions are met	Credentials + requirements validated	If not fulfilled → onboarding rejection
STEP 7 – Membership Credential issuance (DSI B)			
DSI B (Onboarding DSI / Intermediary / EAA Provider)	Issues Dataspace Membership Credential specific to DSI B		—
DSI B (Onboarding DSI / Intermediary / EAA Provider/ Issuer)	Sends Membership Credential to wallet	Wallet capable of receiving credentials	Delivery failure → retry
Step 8 – Storage in wallet			
User /Wallet	Stores Membership Credential (DSI B) alongside existing credentials	Wallet storage capability	Storage failure → retry or error

3.3 Scenario 1 – User story 3

Issue credential to previously onboarded DSI members

Actor	Interpretation or reference	Dependencies	Variations and exceptions
STEP 1 – Initiate Onboarding in DSI C			
User (legal persons)	User opens the DSI C portal after signing in with traditional means and visits the “My account” page	Wallet available and operational, EBW-OID available	
User (legal persons)	User pushes the “Get My Membership” credential		
DSI C (Onboarding DSI / Intermediary / EAA Provider)*	Receives request to issue membership credential and runs internal check to see if all data is available (eg latest rulebook signed)	DSI onboarding interface available	The onboarding request may be automatically rejected/labelled as unsuccessful if the DSI onboarding platform is unavailable
*The parts that are in bold indicate the role that the actor plays in this step, since this actor can play multiple roles across the scenario based on the ARF role definitions .			
STEP 2 – Request and presentation of credentials			
DSI C (Onboarding DSI / Intermediary / EAA Provider)	Requests EBW-OID credential from the user	Wallet + credential support	Additional attributes may be requested depending on DSI
User of Wallet Unit (legal persons)	Presents EBW-OID and Membership Credential from wallet	EBW-OID Credential stored in wallet	Missing credentials → issuance cannot proceed
STEP 3 – Identity Credential verification by DSI C as Relying Party			
DSI C (Onboarding DSI / Intermediary / EAA Provider)	Verifies credential integrity and content (signature, validity)	VC/VP verification capability	Invalid credentials → onboarding rejected

DSI C (Onboarding DSI / Intermediary / EAA Provider)	Verifies the issuer and credential status	Status list and Trusted list from PR	
STEP 4 – Decision on identity and trust by DSI C as Relying Party			
DSI C (Onboarding DSI / Intermediary / EAA Provider)	Evaluates whether the identity credential (EBWOID) is valid and the issuer is trusted	Successful verification	If not valid → onboarding rejected
DSI C (Onboarding DSI / Intermediary / EAA Provider)	If valid, proceeds with issuance of the membership credential	Identity verified	—
STEP 5 – Membership Credential issuance (DSI C)			
DSI C (Onboarding DSI / Intermediary / EAA Provider)	Issues Dataspace Membership Credential specific to DSI C		—
DSI C (Onboarding DSI / Intermediary / EAA Provider/ Issuer)	Sends Membership Credential to wallet	Wallet capable of receiving credentials	Delivery failure → retry
Step 6 – Storage in wallet			
User /Wallet	Stores Membership Credential (DSI C) alongside existing credentials	Wallet storage capability	Storage failure → retry or error

4. Roles and participants

4.1 Scenario roles and participants

The table below describes the roles relevant to this scenario and lists which partners will play each role in piloting it. Note that the roles primarily active in the use case are mentioned.

Primary role	UC partner Name	Country
1. User of EUDI Wallet		
	Farmers, companies participating in DjustConnect (Belgium)	BE
	Farmers, companies participating in DADS(Slovenia)	SI
	Farmers, companies participating in Tritom (Finland)	FI
2. Authentic sources		
	National business registers / VAT registries (via identity providers)	BE / SI / FI
	QTSP group from WP4 for mock data: Spherity, DigIdentity	BE / SI / FI
3. Relying party / Intermediary		
	ILVO – DjustConnect platform	BE
	ITC – DADS platform	SI
	Dataspace Europe – Tritom platform	FI
4. EAA Provider		
	ILVO – DjustConnect platform	BE
	ITC – DADS platform	SI
	Dataspace Europe – Tritom platform	FI

4.2 Additional roles and partners

The table below describes which partners that primarily work in WP4 participate in piloting this scenario.

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	Spherity	DE	BW
	Digidentity	NL	NW/BW
	LutraLabs	SI	BW
2. PID Provider	Digidentity (mock) / WP4 support Spherity (mock)	NL / BE / / FI	
3. Trusted list registrar	LotE to be set up by UC lead in LoTL provided by WP4 (Raidam)	Webuild Global	
4. QEAA provider	Not used in MVP (future role)		
5. Pub-EAA provider	Not explicitly defined in MVP		
6. QES provider/ QTSP	Signicat (potential), Digidentity	NL / NO	
7. Attestation Scheme Provider	Credential Catalogue provided by WP4 (Siros)	Webuild Global	

4.3 Target country combinations

The table below shows which countries intend to pilot the scenario with each other.

Relying Party country	Issuing country					
		SI	BE	FI		...
	SI					
	BE					
	FI					
	...					

4.4 Requirements

The main requirements for each of the involved roles are included as an Annex.

5. Attestations

5.1 Introduction

This section summarizes the attestations used to pilot the scenario. Attestations can be either created within the use case (by the scenario partners) or provided by other use cases or working groups.

This section clarifies which attestations will be of what type. In contrast, the details of each attestation to be created within the scenario will be described in attestation rulebooks as separate documents.

5.2 Attestations to be provided by other UCs/WGs/scenario

Attestation name	Short description	To be provided by	For Countries	Requirements
EBW-OID	EU Business Wallet Owner Identification Data (previously "Legal Person Identification Data")	WP4 PID Providers group	SI, BE, FI	Must be a valid and verifiable Legal Person identifier that makes it possible to identify and authenticate an "economic operator"
VAT ID	An identifier of a Legal Entity (comparable to the EBW-OID). It refers to the official,	BU3 (design) QTSP	SI, BE, FI	Must be a valid and verifiable VAT number r that makes it possible to

nationally recognised registration number of a company or organisation, issued by a public authority (Business Registry) and uniquely identifying the legal entity within a Member State.	(mocked attestations)	identify and authenticate an "economic operator"
---	-----------------------	--

5.3 Created attestations in the scenario

Attestation name	Short description	For Countries	Applicable domain standards
Dataspace Membership Credential	Verifiable credential confirming that a participant is a member of a specific data sharing platform (DSI) or a dataspace. Includes membership-related attributes such as holderIdentifier, memberOf, roles and (dataspace) governance rulebook adherence.	SI, BE, FI (EU wide)	W3C Verifiable Credentials, DSSC Blueprint, Relevant EUDI Wallet and eIDAS 2.0 specifications, Sitra Rulebook

There is an updated description of the attestation as we are focusing in the MVP scenario on a single DS Membership credential. group: [SC2 MVP Scenario 1 Membership credential description](#).

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organisational/technical requirements for each role in the scenario.

Primary role	Specific requirement	MoSCoW
User of EUDI Wallet	MUST be able to store and present Dataspace Membership Credential from the wallet	MUST
	MUST be able to present identity attributes (EBW-OID, VAT) during onboarding	MUST
	MUST be able to consent to sharing credentials with DSIs during onboarding	MUST
	SHOULD be able to reuse credentials across multiple DSIs without re-registration if rulebooks are compatible	SHOULD
Authentic sources	MUST provide authoritative identity data for Legal Persons (e.g. VAT, business registration data (EBW-OID))	MUST
	MUST allow verification of identity attributes used during onboarding (EBW-OID, VAT)	MUST
	SHOULD support cross-border verification of identity attributes	SHOULD
Relying party (DSIs: ILVO, ITC, DSE)	MUST accept Dataspace Membership Credential issued within the 'mini' dataspace "Agri-X"	MUST

	MUST verify credential integrity (signature, validity, issuer trust)	MUST
	MUST support onboarding based on credential reuse (without full re-registration)	MUST
	SHOULD support additional onboarding requirements (e.g. rulebook acceptance) only where necessary	SHOULD
Intermediary (DSIs acting as onboarding providers)	MUST perform identity verification based on EBW-OID and VAT before onboarding approval	MUST
	MUST present the dataspace governance rulebook to participants	MUST
	MUST issue DS Membership credential for dataspace	MUST
	SHOULD align onboarding requirements across DSIs to enable reuse	SHOULD
EUDI Wallet provider	MUST support storage and presentation of W3C Verifiable Credentials (VC/VP)	MUST
	MUST support Dataspace Membership Credential formats (JSON-LD, SD-JWT) used in this scenario	MUST
	MUST support issuance and presentation flows compatible with participating DSIs	MUST
	SHOULD support interoperability across wallet providers used in BE, SI, FI	SHOULD
(L)PID Provider	MUST provide EBW-OID (or equivalent identifier) for Legal Persons in BE, SI, FI	MUST

	MUST ensure identifiers can be used for onboarding across DSIs in the mini dataspace	MUST
	MUST ensure identifiers can be issued to and used within participating wallets	MUST
	SHOULD support cross-border recognition of identifiers	SHOULD
Trusted list registrar	SHOULD list the DSIs as issuer of the DS Membership credential (LotE)	SHOULD
QEAA provider	No requirements defined for MVP Scenario 1 (QEAs not used)	
Pub-EAA provider	No specific requirements defined for MVP Scenario 1	
EAA provider	MUST issue Dataspace Membership Credential after accepting the dataspace governance rulebook and based on verified identity	MUST
	MUST ensure credentials follow agreed schema and attestation rules	MUST
	MUST ensure credentials are issuable to participating wallets	MUST
	SHOULD ensure interoperability of credentials across DSIs in BE, SI, FI	SHOULD

. QES provider	SHOULD support issuance of cryptographic credentials or signatures used in credential validation	SHOULD
	SHOULD support integration with authentic sources for identity verification (if applicable)	SHOULD
	COULD support future issuance of qualified attestations (e.g. EUCC)	COULD

Aspect	QEAs	EAs
Issuer	Qualified Trust Service Provider (QTSP)	Any trusted entity (e.g. DSI)
Regulation	Strict (eIDAS)	Flexible
Legal recognition	High (EU-wide)	Context-dependent
Trust basis	Legal framework	EUDI Framework LotE, Credential Catalogue
Implementation complexity	High	Lower
Examples	EUCC, official registries	Data space Membership Credential

webuild-consortium / SC5

Q

Type / to search

Code

Issues

Pull requests 1

Agents

Actions

Projects

Security and quality

SC5 / Scenario / Description.md

kjorlaug

Moved pilot participants to scenario description

41ef524 · 3 weeks ago

History

371 lines (281 loc) · 22.5 KB

SC5 — eInvoicing: Scenario Specifications

WE BUILD consortium | WP2 — UC SC5

Date	2026-05-24
Version	1.0
Status	Final
Author(s)	Rune Kjørlaug - OpenPeppol

Index

1. [Introduction](#)
- 1.1 [Objectives of this document suite](#)

◦ 1.2 [Scenario overview](#)

◦ 1.3 [Reference documents](#)
2. [Common concepts and architecture](#)
- 2.1 [The Peppol 4-corner model](#)

◦ 2.2 [Trust enhancement through attestations](#)

- [2.3 Common pre-conditions \(Peppol-based scenarios\)](#)
- [2.4 WE BUILD pilot context and qualification model](#)
- [2.5 System-to-system wallet interactions](#)
- 3. [Roles and participants](#)
 - [3.1 Actor model summary](#)
 - [3.2 Pilot participants](#)
 - [3.3 Additional roles and partners](#)
 - [3.4 Target country combinations](#)
 - [3.5 Requirements](#)
- 4. [Attestations](#)
 - [4.1 Introduction](#)
 - [4.2 Attestations provided by other UCs/WGs](#)
 - [4.3 Attestations created in SC5](#)
- [Annex A — Abbreviations](#)

1. Introduction

1.1 Objectives of this document suite

This document suite describes the scenario specifications for Use Case SC5 (eInvoicing) in Work Package 2 of the WE BUILD consortium. It provides detailed information on the processes to be piloted, the attestations used, the actors involved, and the dependencies on other use cases and work packages.

The suite is organised as follows:

File	Content
Introduction (this file)	Common introduction, concepts, roles, attestations and abbreviations shared across all scenarios
Scenario 1	Scenario 1 — Supplier pre-approval
Scenario 2	Scenario 2 — Service Provider authorization
Scenario 3	Scenario 3 — Service Provider authorization verifiable by Tax

	Administration
Scenario 4	Scenario 4 — Direct eInvoicing between Business Wallets
Scenario 5	Scenario 5 — Peppol enhancements

This suite is a product of the Specification Phase of the WE BUILD LSP and serves as a key input to solution development and pilot preparation.

1.2 Scenario overview

The SC5 scenarios share a common foundation where applicable. Scenarios 1, 2, 3 and 5 are built on the Peppol network's 4-corner model, enhanced with European Business Wallet (EBW) attestations to strengthen trust and enable machine-verifiable authorization. Scenario 4 uses the "reference attestation" concept to enable the Buyer's Business Wallet to pull the eInvoice from the Sender, independent on transfer mechanism.

ID	Scenario name	Attestation(s)	Transport	MVP
1	Supplier pre-approval	Approved Supplier	Peppol AS4	Y
2	Service Provider authorization	Authorized Service Provider	Peppol AS4	Y
3	SP authorization verifiable by Tax Administration	Authorized Service Provider	Peppol AS4 + TA API	MVP+
4	Direct eInvoicing between Business Wallets	eInvoice Attestation	OID4VP/DCQL	Y
5	Peppol enhancements	As per scenarios 1, 2, 3	Peppol AS4 + ERDS/QRDS	MVP+

Scenarios 1, 2 and 4 are part of the Minimum Viable Product (MVP). Scenarios 3 and 5 are designated MVP+.

Common pilot flows

The pilot will use real data where possible — real company names and real identifiers — but in the test environment provided by WE BUILD. The attestations and wallet instances used will not have any legal effect.

For Scenarios 1, 2, 3 and 5, several Peppol Service Providers participate as Relying Parties, each serving end-user customers across multiple EU Member States. This makes country coverage inherently broad and flexible — the scenarios are not tied to a fixed pair of countries but reflect the multi-country reality of the participating SPs' customer bases. For Scenario 4, direct wallet-to-wallet exchange is piloted between Robert Bosch (DE) and Sphereon (NL).

Participant details are documented per scenario.

1.3 Reference documents

WE BUILD project documents

- SC5 Stock Taking document v1.0 (11/12/2025)
- [WE BUILD Architecture & Integration Blueprint \(D4.1\)](#)
- [WE BUILD Architectural Decision Records \(ADRs\)](#) — in particular:
 - ADR: Provide EBWOID as a stable minimal basis
 - ADR: Attestation Revocation Mechanism
 - ADR: Specify PID and eAA formats
 - ADR: Baseline protocols
 - ADR: Deliver business wallet data using QERDS
- [WE BUILD Conformance Specification cs-01: Credential Issuance](#)
- [WE BUILD Conformance Specification cs-02: Credential Presentation](#)
- [WE BUILD Attestation Rulebooks catalog](#)
- eInvoice Attestation specification (v0.5 final draft)

Regulatory and standards

- ARF (version to be confirmed)
- eIDAS Regulation (amended by 2024/1183) and relevant Implementing Acts
- EBW Regulation proposal
- Peppol BIS Billing 3.0
- Peppol AS4 Profile

- EN 16931 (European e-invoicing standard)
- EWC RB001 — LPID Rulebook (predecessor; EBWOID rulebook to be published under WE BUILD)
- EWC RB002 — EUCC Rulebook
- OpenID4VCI (latest version)
- OpenID4VP (latest version)
- SD-JWT-VC specification
- W3C Verifiable Credentials Data Model (VCDM)
- IETF Token Status List (revocation)
- ETSI TS 119 602 — List of Trusted Entities (LoTE)

2. Common concepts and architecture

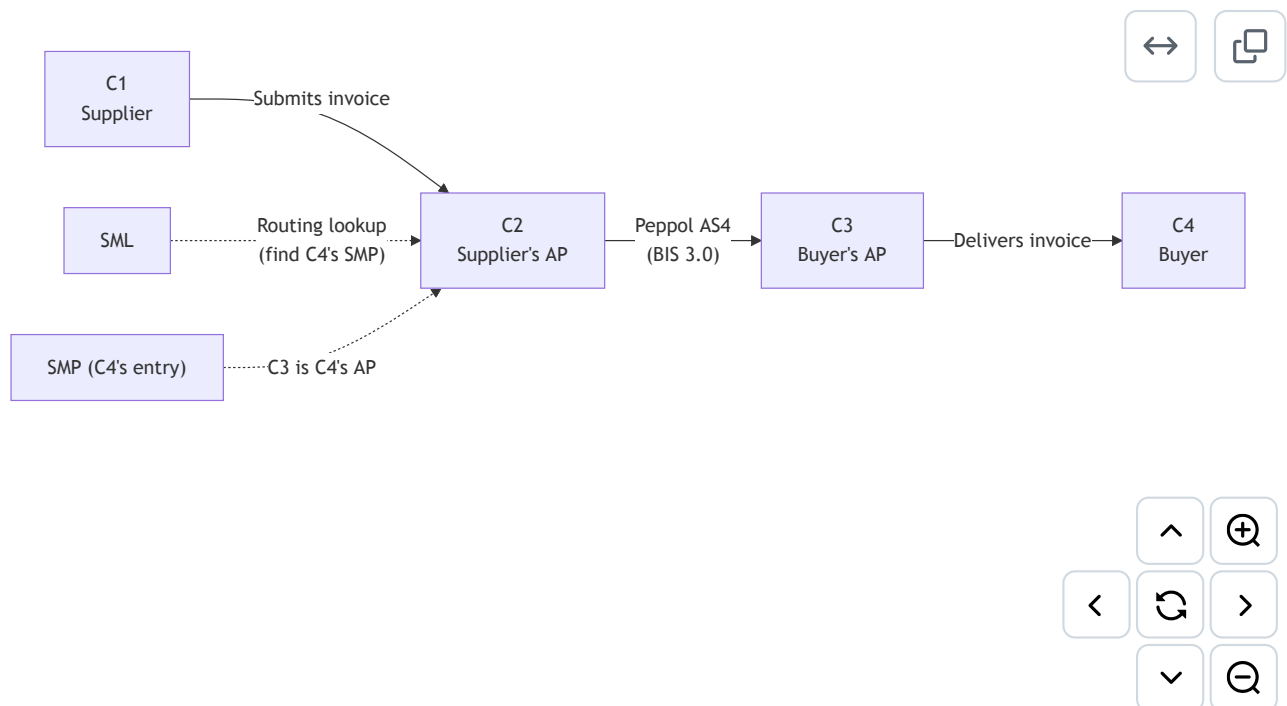
2.1 The Peppol 4-corner model

All Peppol-based scenarios (1, 2, 3 and 5) operate within the standard 4-corner model:

- **C1** — Sending end user (Supplier): creates and sends the invoice
- **C2** — Sending Service Provider (Access Point): transmits the invoice on behalf of C1
- **C3** — Receiving Service Provider (Access Point): receives the invoice on behalf of C4
- **C4** — Receiving end user (Buyer): receives and processes the invoice

Invoice exchange follows the Peppol BIS 3.0 format over AS4. C2 resolves the delivery endpoint for a given invoice by querying the SML to find C4's SMP, which returns C3 as the AP authorised to receive on C4's behalf. SC5 does not change the transport layer — it adds verifiable trust signals at key decision points in the flow.

Note on receipts (MLR/MLS): The current Peppol specification does not mandate an application-level receipt from C4 back to C1 confirming that an invoice has been processed or accepted. The AS4 transport acknowledgement between C3 and C2 is the only standardised confirmation. Work is ongoing within the Peppol community on **Message Level Response (MLR)** and **Message Level Status (MLS)** to introduce a standardised business-level receipt mechanism. SC5 should monitor this work, as a future MLR/MLS could carry attestation-related metadata — for instance, confirming that C4 accepted the invoice against a valid Approved Supplier attestation — and would close a significant gap in the end-to-end trust chain.



2.2 Trust enhancement through attestations

The core idea of SC5 (Peppol-based scenarios) is that the invoice itself remains

[SC5](#) / [Scenario](#) / [Description.md](#)

[↑ Top](#)

Preview

Code

Blame



Raw



Two new attestation types are introduced for the Peppol-based scenarios:

- **Approved Supplier attestation** — issued by a Buyer (C4) to a Supplier (C1), proving the existence of a trusted and acknowledged contractual relationship between the two legal entities. The parties are implicitly determined by the Wallet

Instances involved, each bound to a verified legal entity. The attestation may be grounded in a public authoritative source (e.g. a contract award notice on TED) or in contractual evidence or buyer acknowledgement.

- **Authorized Service Provider attestation** — issued by a company (C1 or C4) to its Service Provider (C2 or C3), proving that the SP is authorised to act on the company's behalf for one or more explicitly defined functions, including sending or receiving electronic invoices, and submitting VAT or transaction data to tax authorities. Legal identity of the mandating business and the SP is not asserted in the attestation itself; it is established through separate legal person attestations (e.g. EUCC).

Both attestation types are Electronic Attestations of Attributes (EAA) in the sense of eIDAS 2.0. Whether they need to be Qualified (QEAA) is a working assumption pending further analysis.

Scenario 4 introduces a third type:

- **eInvoice Attestation** — a verifiable representation of an invoice exchange event, issued by the Supplier's Business Wallet, binding invoice content (via a payload hash) to a cryptographic signature associated with the Supplier's legal-person identity. In the regulation this is called a reference attestation.

2.3 Common pre-conditions (Peppol-based scenarios)

The following pre-conditions apply across all Peppol-based SC5 scenarios (1, 2, 3 and 5):

1. C1 (Supplier) and C4 (Buyer) are registered Peppol participants with entries in the SMP. C4's SMP entry records C3 as the Access Point authorised to receive documents on C4's behalf; C1's SMP entry records C2 similarly. C2 and C3 do not have their own SMP entries — they are service providers acting on behalf of their clients.
2. C2 and C3 are certified Peppol Access Points.
3. European Business Wallets are available and operational for C1, C4, and the SPs as applicable; wallet providers have passed ITB testing.
4. EBWOID attestations are issued to the relevant business wallets by WP4-designated EBWOID providers.
5. WP4 trust infrastructure is operational: the WE BUILD LoTL, WE BUILD Trusted Lists, and relying party registration are available.

6. The Approved Supplier and Authorized Service Provider attestation schemas and rulebooks are defined (to be delivered by SC5 in coordination with the WP4 semantics group and published in the WE BUILD Attestation Rulebooks catalog).
7. Issuers, Holders and Relying Parties implement the WE BUILD Conformance Specifications cs-01 (issuance) and cs-02 (presentation) for the above attestation types.
8. Revocation infrastructure for SC5 attestations is operational, using the IETF Token Status List mechanism as mandated by the WE BUILD ADR on Attestation Revocation.

2.4 WE BUILD pilot context and qualification model

SC5 operates within the WE BUILD pilot environment, which is a large-scale test environment and not the final eIDAS production ecosystem. This has specific implications for how trust and qualification are handled in the pilot, as documented in the Blueprint (D4.1, section 1.2.1).

WE BUILD does not	WE BUILD does
Issue eIDAS-qualified attestations (QEAA)	Define WE BUILD QEAA focused on technical interoperability
Use the EC List of Trusted Lists (LoTL)	Provide a WE BUILD LoTL
Use MS Trusted Lists	Provide WE BUILD Trusted Lists with input from supervisory bodies where available
Issue eIDAS RP access certificates	Issue WE BUILD RP access certificates
Reach production-level legal liability	Operate within the WE BUILD agreement and trust framework

Consequently, any reference in this document suite to "QEAA" in the pilot context means **WE BUILD QEAA**: a technically interoperable credential that follows eIDAS patterns and passes the Interoperability Testbed (ITB), but does not carry eIDAS legal qualification.

All SC5 implementations — wallet providers, issuers, relying parties — must pass the ITB before participating in pilots. The WBCS (cs-01 for issuance, cs-02 for presentation) define the technical requirements that implementations must conform to.

2.5 System-to-system wallet interactions

The Peppol-based SC5 scenarios involve machine-to-machine flows between backend systems (Access Points), not direct end-user interactions. As noted in the Blueprint (section 4.5), enterprise and system-to-system wallet interactions are fully supported: credential issuance and presentation may be initiated by backend systems, while the same trust framework, credential formats and verification mechanisms apply as in user-driven flows.

This is directly applicable to SC5: C2 acts as a Relying Party in a fully automated pipeline when it checks attestations on incoming invoice submissions. The OpenID4VP exchange between C1's EBW and C2, or between C2 and C3, is a system-to-system interaction with no human-in-the-loop required at runtime.

3. Roles and participants

3.1 Actor model summary

Business actor	ARF role	Scenarios
Buyer (C4)	Issuer (Approved Supplier; Authorized SP for C3)	1, 2, 3, 5
Supplier (C1)	Holder/Presenter (Approved Supplier); Issuer (Authorized SP for C2, eInvoice to C4)	1, 2, 3, 4, 5
Supplier's AP (C2)	Relying Party (Approved Supplier); Holder/Presenter (Authorized SP)	1, 2, 3, 5
Buyer's AP (C3)	Relying Party (Authorized SP from C1/C2); Holder/Presenter (Authorized SP from C4)	2, 3, 5
Tax Authority (MS A / MS B)	Relying Party (Authorized SP attestation for tax reporting)	3
Supplier		

(Business Wallet)	Issuer (eInvoice Attestation)	1, 2, 3, 4, 5
Buyer (Business Wallet)	Holder/Relying Party (eInvoice Attestation)	1, 2, 3, 4, 5
QTSP	Trust service provider (QESeal, ERDS/QRDS)	5

3.2 Pilot participants

Participant details are specified in each scenario file. The table below gives an overview per scenario.

Scenario	Relying Parties	Issuer countries
1	B2BRouter (ES), ILYDA (GR), Banqup (BE), Ledger Leopard (NL), Datev (DE)	FR, BE, NL, DE, GR, ES, SE
2	B2BRouter (ES), ILYDA (GR), GSIS (GR), Banqup (BE), Ledger Leopard (NL), Datev (DE)	FR, BE, NL, DE, GR, ES, SE
3	TBD	TBD
4	Bosch (DE)	DE, NL
5	TBD	TBD

3.3 Additional roles and partners

Primary role	UC partner name	Country	Wallet
Tax authority (Supplier side)	TBD		
Tax authority (Buyer side)	TBD		
EU Business Wallet provider	Sphereon & Credenco	NL	
EUCC/LPID Provider	(out of scope)		
Trusted list registrar	IDunion SCE	DE	

QEAA provider	(out of scope)		
Pub-EAA provider	(out of scope)		
EAA provider	Datev	DE	
QES provider	ValidatedID, Banqup	ES, BE	

3.4 Target country combinations

Peppol-based scenarios (1, 2, 3, 5)

Coverage is determined by the customer base of the participating Service Providers and is not limited to fixed country pairs. Member States involved: **FR, BE, NL, DE, GR, ES, SE.**

Scenario 4

Issuer (Supplier Wallet)	Relying Party (Buyer Wallet)
DE, NL	DE

3.5 Requirements

The main functional, organizational and technical requirements for each role are included in Annex 1 of each individual scenario file.

4. Attestations

4.1 Introduction

SC5 introduces three new attestation types that do not currently exist in the EUDI ecosystem or any other standard. This section provides an overview. Full schemas and claim definitions are included in the relevant scenario specification files and will be detailed in dedicated attestation rulebooks.

SC5 reuses the EBWOID (for identifying companies) as a dependency from WP4, but the new attestation types must be specified, schematized and governed by SC5 in coordination with the WP4 semantics group.

4.2 Attestations provided by other UCs/WGs

Attestation name	Short description	To be provided by	Requirements
EBWOID	European Business Wallet Organisation Identifier — the cross-border minimum organisation identifier in the WE BUILD ecosystem, providing a stable, wallet-bound basis for identifying legal persons across Member States. Successor to the LPID concept from earlier LSPs.	WP4 — PID & EBWOID Providers group	Must include: EUID (ISO 6523-compliant), legal name, registered address, VAT number (where applicable). Used to uniquely identify C1, C2, C3 and C4 in attestation subject/issuer fields. Availability in all piloting Member States is a critical path dependency.
EUCC (optional)	EU Company Certificate; richer set of company attributes	BU2	Optional enhancement for richer verification; not required for MVP.

4.3 Attestations created in SC5

Approved Supplier attestation (Scenarios 1, 4, 5)

Attribute	Value
Issuer	Buyer (C4)
Holder / subject	Supplier (C1)
Relying Party	Supplier's AP (C2)

ARF attestation type	EAA (QEAA pending analysis)
Credential format	SD-JWT-VC

The parties (Buyer and Supplier) are implicitly determined by the Wallet Instances involved and are not embedded as explicit identity claims in the attestation. Legal identity is established through separate attestations (EBWOID).

Key attributes (from attestation spec):

Attribute	M/O	Description
relationship_id	M	Unique identifier of the acknowledged relationship
relationship_type	M	Type of relationship (code list: contractual , framework_agreement , public_contract_award , private_contract , buyer_acknowledgement)
relationship_status	M	Current status — SHALL be active for invoicing trust decisions
relationship_start_date	M	Start date of the acknowledged relationship
relationship_end_date	O	End date of the relationship, if applicable
authoritative_source	O	Reference to the authoritative source or evidence (Source reference object)

Authorized Service Provider attestation (Scenarios 2, 3, 5)

Attribute	Value
Issuer	Company (C1 or C4)
Holder / subject	Service Provider (C2 or C3)
Relying Party	Counterpart AP (C3 or C2); Tax Authority (Scenario 3)
ARF attestation type	EAA (QEAA pending analysis)

Credential format

SD-JWT-VC

Legal identity of the mandating business and the service provider is NOT asserted in this attestation — it SHALL be established through separate legal person attestations (e.g. EBWOID). The mandating business is referenced via a structured object containing its VAT number and country code, sufficient for relying party processing.

Key attributes (from attestation spec):

Attribute	M/O	Description
mandate_id	M	Unique identifier of the mandate
mandate_type	M	Type of mandate (code list: <code>invoice_sending</code> , <code>invoice_receiving</code> , <code>vat_reporting</code> , <code>transaction_reporting</code>)
mandate_start_date	M	Start date of the mandate
mandate_end_date	O	End date of the mandate, if applicable
mandating_business	M	Reference to the mandating business (Mandating business reference object: <code>vat_number</code> M, <code>country_code</code> M, <code>business_identifier</code> O)
mandate_scope	M	Scope within which the SP is authorised to act (Mandate scope object: <code>scope_type</code> M from code list <code>einvoicing</code> / <code>vat_reporting</code> / <code>regulatory_reporting</code> ; <code>vat_reporting_scope</code> O)
authority_source	O	Reference to the authentic source supporting the mandate (Authority reference object)

eInvoice Attestation (Scenario 4)

Attribute	Value
Issuer	Supplier (via Supplier Wallet)
Holder / subject	Buyer Wallet
Relying Party	Buyer Wallet

ARF attestation type	EAA
Credential format	SD-JWT-VC
Applicable domain standards	EN16931-UBL and/or Peppol BIS3

Annex A — Abbreviations

Abbreviation	Definition
AP	Access Point
ARF	Architecture Reference Framework
B2B	Business-to-Business
B2G	Business-to-Government
BIS	Business Interoperability Specification
EAA	Electronic Attestation of Attributes
EBW	European Business Wallet
EUID	European Unique Identifier
EUCC	EU Company Certificate
KYB	Know Your Business
KYS	Know Your Supplier
ADR	Architectural Decision Record
CIUS	Core Invoice Usage Specification
ERDS	Electronic Registered Delivery Service
EBWID	European Business Wallet Organisation Identifier
ITB	Interoperability Testbed
LoTL	List of Trusted Lists
LoTE	List of Trusted Entities

UBL	Universal Business Language
LSP	Large Scale Pilot
MVP	Minimum Viable Product
OpenID4VCI	OpenID for Verifiable Credential Issuance
OpenID4VP	OpenID for Verifiable Presentations
PKI	Public Key Infrastructure
QEAA	Qualified Electronic Attestation of Attributes
QERDS	Qualified Electronic Registered Delivery Service
QES	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
QTSP	Qualified Trust Service Provider
SD-JWT-VC	Selective Disclosure JWT Verifiable Credential
SML	Service Metadata Locator
SMP	Service Metadata Publisher
SP	Service Provider
TDD	Tax Data Document
VAT	Value Added Tax
VCDM	Verifiable Credentials Data Model
ViDA	VAT in the Digital Age
WP	Work Package
WBCS	WE BUILD Conformance Specification

webuild-consortium / SC5

Q

Type / to search

Code

Issues

Pull requests1

Agents

Actions

Projects

Security and quality

SC5 / Scenario / Scenario1.md

kjorlaug

Moved pilot participants to scenario description

41ef524 · 3 weeks ago

History

167 lines (126 loc) · 10.9 KB

Preview

Code

Blame

Raw

SC5 — Scenario 1: Supplier Pre-Approval

WE BUILD consortium | WP2 — UC SC5

Date	2026-05-24
Version	1.0
Status	Final
Author(s)	Rune Kjørlaug - OpenPeppol

Part of the SC5 eInvoicing specification suite. Read [Introduction.md](#) for common concepts, roles, attestations and abbreviations.

Index

- [Introduction](#)
- [Pre-conditions](#)
- [Main flow](#)
- [Detailed scenario flow](#)

5. [Additional flows](#)
 6. [Challenges and barriers](#)
 7. [Working assumptions](#)
- [Annex 1 — Requirements for scenario roles](#)

1. Introduction

Scenario 1 introduces the **Approved Supplier attestation** as a mechanism for a Buyer (C4) to pre-approve a Supplier (C1) and make this approval verifiable at the Service Provider level (C2). When C1 submits an invoice, C2 can verify — before transmitting — that C1 holds a valid approval from C4. This prevents unauthorized or fraudulent invoices from entering the Peppol network on behalf of buyers who have not established a commercial relationship with the sending supplier.

This scenario establishes the foundational buyer-supplier trust relationship and is the primary **MVP** scenario.

Participants

The participating Relying Parties (C2) are Peppol Service Providers, each serving end-user customers (C4 — Issuers of the Approved Supplier attestation) across multiple EU Member States. Country coverage is therefore flexible and determined by the SP's customer base.

Role	Organisation	Country
Relying Party (C2)	B2BRouter	ES
Relying Party (C2)	ILYDA	GR
Relying Party (C2)	Banqup	BE
Relying Party (C2)	Ledger Leopard	NL
Relying Party (C2)	Datev	DE

Countries of Issuers (C4): FR, BE, NL, DE, GR, ES, SE

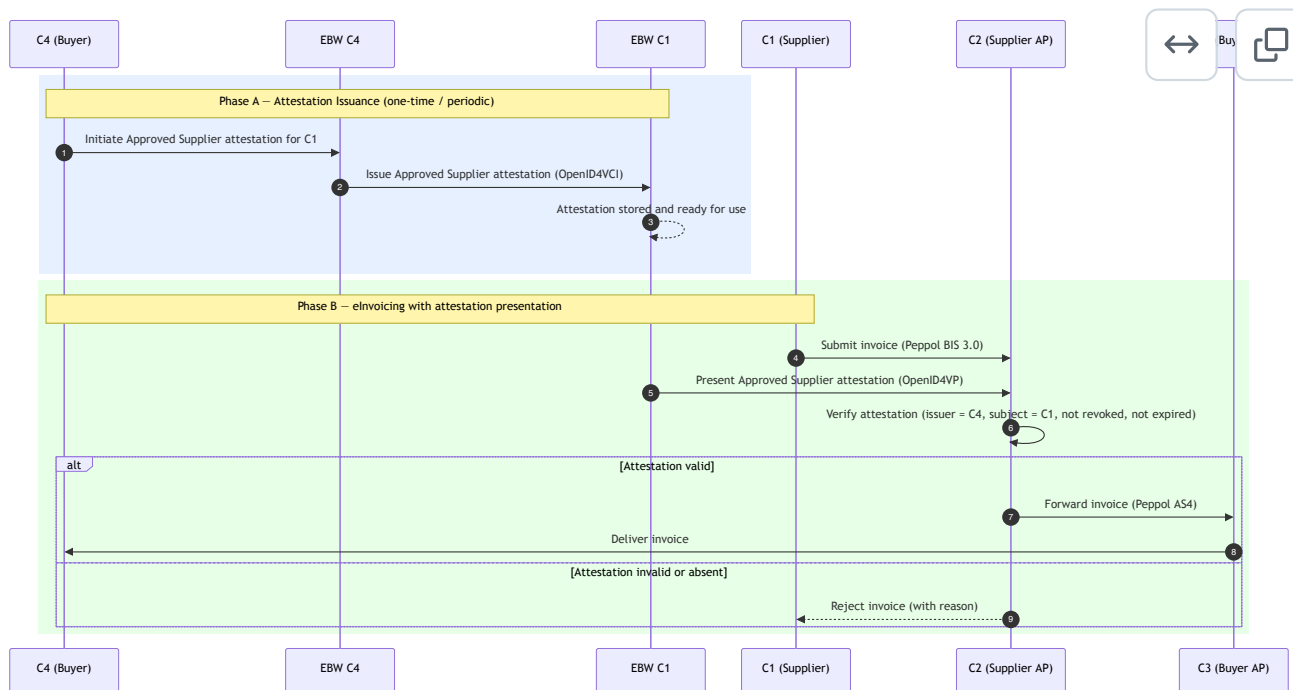
2. Pre-conditions

In addition to the common pre-conditions (SC5_Introduction.md, section 2.3):

1. C4 has an operational EBW capable of issuing the Approved Supplier attestation.
2. C1 has an EBW capable of receiving and presenting the Approved Supplier attestation.
3. C2 is a Relying Party capable of verifying the Approved Supplier attestation via OpenID4VP.
4. The Approved Supplier attestation schema is available and accepted by all parties.
5. C4 has established a commercial relationship with C1 outside of the wallet system (e.g. via a procurement process) and is ready to attest to it.

3. Main flow

The flow consists of two phases: an **attestation issuance phase** (typically a one-time or periodic activity) and the **invoice submission phase** (recurring).



4. Detailed scenario flow

Step	Actor	Description	Dependencies	Variations / exceptions
A.1	C4	C4 initiates the issuance of an Approved Supplier attestation for C1 through their EBW interface. The attestation identifies C1 (via	EBW OID for C1 must be resolvable by C4	C4 may issue the attestation for a limited validity period or with product/category scope

		EBWOID / EUID) as an approved supplier of C4.		
A.2	EBW C4 → EBW C1	The EBW of C4 (acting as Issuer) issues the attestation to the EBW of C1 using OpenID4VCI. The attestation is signed by C4 and bound to C1's wallet.	OpenID4VCI interoperability between wallets; Approved Supplier schema available	Batch issuance for multiple suppliers; delegation to procurement platform
A.3	EBW C1	C1's EBW stores the attestation. C1 is notified.	—	C1 may have multiple Approved Supplier attestations from different buyers
B.1	C1	C1 creates the invoice in Peppol BIS 3.0 format and initiates submission to C2. As part of the submission handshake, C1 presents the Approved Supplier attestation for the relevant buyer (C4) via OpenID4VP.	Approved Supplier attestation in EBW C1; C2 supports OpenID4VP verification	C1 may present the attestation out-of-band (API call separate from invoice submission); scope to be defined
		C2 acts as Relying Party. It verifies: (a) the attestation		

B.2	C2	signature (issuer = C4), (b) the subject matches C1, (c) the attestation is within its validity period, (d) the attestation has not been revoked.	Trust registry accessible to C2; revocation endpoint operational	C2 may cache verification results for a configurable period to avoid repeated checks
B.3a	C2 → C3	If verification succeeds, C2 forwards the invoice to C3 via Peppol AS4. C2 resolves the recipient by looking up C4's Peppol ID in the SML/SMP, which returns C3 as the AP authorised to receive on C4's behalf.	C4 registered in SMP with C3 as receiving AP	C2 may attach attestation metadata to the AS4 message (optional, to be specified)
B.3b	C2 → C1	If verification fails (invalid, absent, expired, revoked), C2 rejects the invoice and returns an error to C1 with a standardized reason code.	—	Reason codes: ATTESTATION_MISSING, ATTESTATION_INVALID, ATTESTATION_EXPIRED, ATTESTATION_REVOKED
B.4	C3 → C4	C3 delivers the invoice to C4 using the agreed delivery	—	—

		mechanism.		
B.5	C3 → C2 → C1	C3 returns an AS4-level acknowledgement to C2; C2 confirms submission to C1. There is no mandatory application-level receipt from C4 back to C1 in the current Peppol specification. Work on MLR/MLS is ongoing and may introduce a standardised receipt mechanism; SC5 should monitor this and consider it for Scenario 5.	—	If MLR/MLS becomes available, C4's receipt could carry attestation-related metadata confirming the invoice was accepted against a valid Approved Supplier attestation

5. Additional flows

Variation/exception	Description
Attestation renewal	If the Approved Supplier attestation has expired, C1 must request renewal from C4 before submitting invoices. C2 rejects the invoice with reason ATTESTATION_EXPIRED.
Multi-buyer scenario	C1 may hold multiple Approved Supplier attestations (one per buyer). C2 selects the relevant one based on C4's Peppol ID present in the invoice.

Attestation revocation

C4 may revoke the attestation at any time (e.g. if the commercial relationship ends). C2 checks revocation status on each submission or on a cached basis.

The following will **not** be piloted in Scenario 1: proximity-based presentation, natural person wallet flows, and changes to the Peppol message format itself.

6. Challenges and barriers

- **No existing Approved Supplier attestation schema:** a new EAA schema and rulebook must be designed from scratch, in coordination with WP4 (semantics group).
- **Wallet interoperability:** the Buyer's EBW and the Supplier's EBW may be from different providers; cross-wallet OpenID4VCI issuance must be tested.
- **C2 integration:** Peppol Access Points must be extended to act as OpenID4VP Relying Parties; this requires changes to their onboarding and operational software.
- **Revocation infrastructure:** revocation of the Approved Supplier attestation must be implemented using the IETF Token Status List, as mandated by the WE BUILD ADR on Attestation Revocation. Attestations with a validity period ≤ 24 hours are exempt from revocation requirements; longer-lived attestations (expected for the Approved Supplier relationship) require a live Token Status List endpoint accessible to C2.
- **EBWOID availability:** issuance of EBWOIDs in all piloting Member States is required before Scenario 1 can be piloted cross-border.

7. Working assumptions

#	Assumption	Rationale
WA1.1	The Approved Supplier attestation is implemented as a non-qualified EAA (not QEAA) for the MVP pilot.	A QEAA mandate would require QTSP involvement and may not be feasible within pilot timelines. This can be escalated for production.

WA1.2	C2 is the primary Relying Party for the attestation; C3 does not verify in Scenario 1.	Placing verification at C2 prevents unauthorized invoices from entering the network at the source. Adding C3 verification is a Scenario 2 / Scenario 5 enhancement.
WA1.3	The attestation is presented via a machine-to-machine OpenID4VP flow, not a browser-based user interaction.	The invoice submission process in Peppol is automated; human-in-the-loop wallet interactions are not appropriate for production invoice flows.
WA1.5	In the WE BUILD pilot, "QEAA" means WE BUILD QEAA (technically interoperable, ITB-tested) rather than eIDAS-qualified.	The WE BUILD pilot environment does not operate within the formal eIDAS certification framework. Production escalation to eIDAS QEAA is a post-pilot decision.

Annex 1 — Requirements for scenario roles



To be completed during specification phase based on partner input.

Primary role	Specific requirement
1. Supplier (C1)	a. Must have an operational European Business Wallet
	b. EBW must support OpenID4VP (presentation)
	c. Must be a registered Peppol participant
2. Buyer (C4)	a. Must have an operational European Business Wallet
	b. EBW must support OpenID4VCI (issuance of Approved Supplier attestation)
	c. Must be a registered Peppol participant
3. Supplier's AP (C2)	a. Must be a certified Peppol Access Point

	b. Must support OpenID4VP as Relying Party (Approved Supplier attestation)
4. EBW provider	a. Must support OpenID4VCI issuance per WBCS cs-01
	b. Must support OpenID4VP presentation per WBCS cs-02
	c. Must pass ITB conformance testing before participating in pilots
5. EBWOID provider	a. As per WP4 requirements
6. Trust registry / Trusted list registrar	a. Must register Issuers of Approved Supplier attestations

SC5 / Scenario / Scenario2.md

168 lines (128 loc) · 8.45 KB

SC5 — Scenario 2: Service Provider Authorization

WE BUILD consortium | WP2 – UC SC5

Date	2026-05-24
Version	1.0
Status	Final
Author(s)	Rune Kjørlaug - OpenPeppol

Part of the SC5 eInvoicing specification suite. Read [Introduction.md](#) for common concepts, roles, attestations and abbreviations.

Index

1. Introduction
2. Pre-conditions
3. Main flow

4. [Detailed scenario flow](#)
 5. [Additional flows](#)
 6. [Challenges and barriers](#)
 7. [Working assumptions](#)
- [Annex 1 — Requirements for scenario roles](#)

1. Introduction

Scenario 2 introduces the **Authorized Service Provider attestation**, issued by a company (C1 or C4) to its Service Provider (C2 or C3 respectively). This allows the receiving AP (C3) to verify — before accepting an invoice — that the sending AP (C2) is legitimately authorized to act on behalf of the sending company (C1).

This adds an additional layer of trust between the APs, complementing Scenario 1's buyer-supplier trust. It guards against unauthorized or misconfigured APs transmitting invoices without a valid mandate from the company they claim to represent.

This is an **MVP** scenario.

Participants

The participating Relying Parties (C3) are Peppol Service Providers, each serving end-user customers (C1/C4 — Issuers of the Authorized Service Provider attestation) across multiple EU Member States. Country coverage is therefore flexible and determined by the SP's customer base.

Role	Organisation	Country
Relying Party (C3)	B2BRouter	ES
Relying Party (C3)	ILYDA	GR
Relying Party (C3)	GSIS	GR
Relying Party (C3)	Banqup	BE
Relying Party (C3)	Ledger Leopard	NL
Relying Party (C3)	Datev	DE

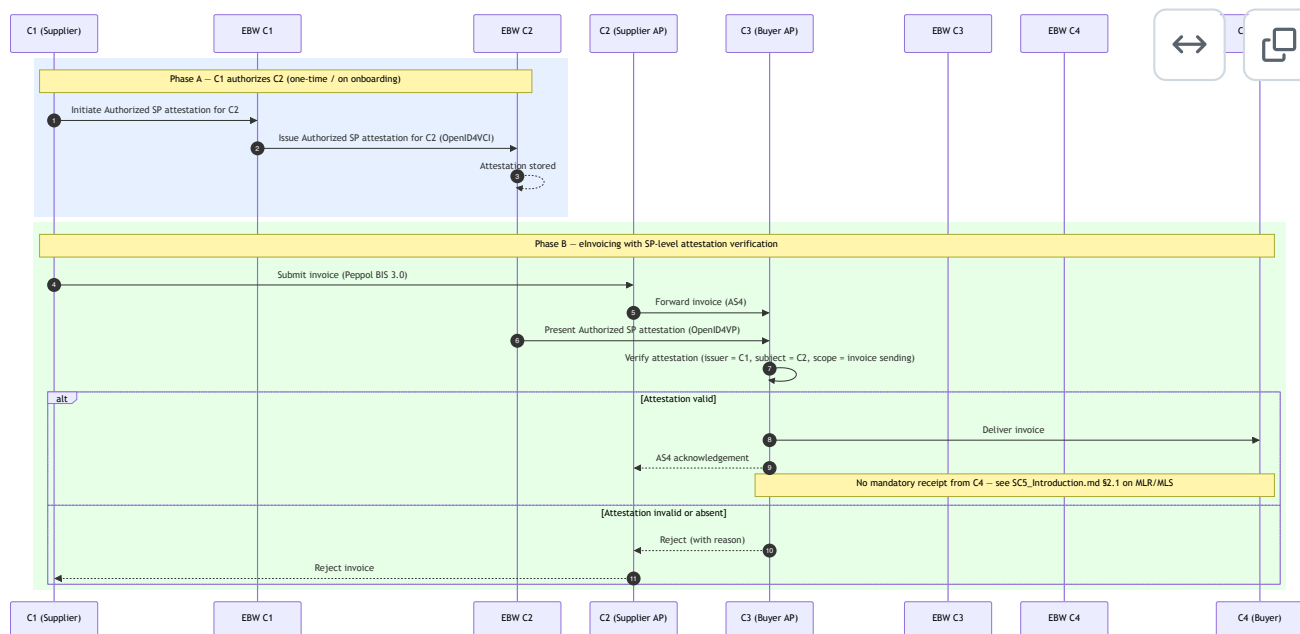
Countries of Issuers (C1/C4): FR, BE, NL, DE, GR, ES, SE

2. Pre-conditions

In addition to the common pre-conditions (SC5_Introduction.md, section 2.3):

1. C1 has an EBW capable of issuing the Authorized Service Provider attestation to C2.
2. C4 has an EBW capable of issuing the Authorized Service Provider attestation to C3 (required if C3-side verification is piloted).
3. C2 and C3 have EBWs (or equivalent wallet-capable infrastructure) to receive and present attestations.
4. C3 is a Relying Party capable of verifying the Authorized Service Provider attestation presented by C2.
5. The Authorized Service Provider attestation schema is available and accepted by all parties.

3. Main flow



4. Detailed scenario flow

Step	Actor	Description	Dependencies	Variations / exceptions
A.1	C1	C1 initiates the issuance of an Authorized SP attestation for C2 via C1's EBW. The attestation certifies that C2 is authorized to send invoices on behalf of C1.	EBW OID for C2 must be resolvable; Authorized SP schema available	Attestation may be scoped to specific document types or Peppol process IDs
	EBW			

A.2	C1 → EBW C2	C1's EBW issues the attestation to C2's EBW via OpenID4VCI.	OpenID4VCI interoperability	—
B.1	C1 → C2	C1 submits invoice to C2 through normal Peppol onboarding channel.	—	Optionally combined with Scenario 1 attestation presentation
B.2	C2 → C3	C2 sends the invoice to C3 via Peppol AS4. As part of the AS4 exchange (or a preceding handshake), C2 presents its Authorized SP attestation to C3 via OpenID4VP.	C3 supports OpenID4VP; trust registry accessible	Timing of attestation presentation (before AS4, during AS4 header, or as separate API call) to be specified
B.3	C3	C3 verifies: (a) attestation issuer = C1, (b) subject = C2, (c) validity period, (d) not revoked, (e) scope covers invoice transmission.	Trust registry; revocation endpoint	C3 may also verify C4 has authorized it (if A' was performed)
B.4a	C3 → C4	If valid, C3 delivers to C4.	—	—
B.4b	C3 → C2	If invalid, C3 rejects with reason code. C2 notifies C1.	—	—

5. Additional flows

Variation/exception	Description
	When C1 changes to a new AP, the old Authorized SP

SP change	attestation must be revoked and a new one issued.
Mutual verification	C2 may request to verify C3's authorization (C4 → C3) before sending. This symmetric trust model may be mandated in Scenario 5.

6. Challenges and barriers

- **Wallet for Service Providers:** APs need EBWs or equivalent infrastructure to hold and present attestations. This is a significant change to current AP software and operational practice.
- **AS4 integration point:** defining where exactly attestation presentation fits into the AS4 message exchange is a key technical design question requiring alignment with the Peppol AS4 profile owners.
- **Schema alignment with Scenario 1:** the Authorized SP attestation schema must be designed to complement the Approved Supplier attestation without creating redundancy.

7. Working assumptions

#	Assumption	Rationale
WA2.1	For the MVP, only the C2-to-C3 verification is piloted (C2 presents attestation from C1 to C3). C3's authorization by C4 is MVP+.	Reduces scope and partner complexity for the MVP. The asymmetric model still provides meaningful fraud prevention.
WA2.2	Attestation presentation by C2 to C3 occurs as a pre-transmission handshake, not embedded in the AS4 message itself.	Avoids changes to the Peppol AS4 message format. The handshake can be an OpenID4VP exchange triggered before the AS4 SUBMIT call.

Annex 1 — Requirements for scenario roles



To be completed during specification phase based on partner input.

Primary role	Specific requirement
1. Supplier (C1)	a. Must have an operational European Business Wallet
	b. EBW must support OpenID4VCI (issuance of Authorized SP attestation)
	c. Must be a registered Peppol participant
2. Buyer (C4)	a. Must have an operational European Business Wallet
	b. EBW must support OpenID4VCI (issuance of Authorized SP attestation to C3)
	c. Must be a registered Peppol participant
3. Supplier's AP (C2)	a. Must be a certified Peppol Access Point
	b. Must have an EBW for holding and presenting Authorized SP attestation
	c. Must support OpenID4VP as Holder/Presenter
4. Buyer's AP (C3)	a. Must be a certified Peppol Access Point
	b. Must support OpenID4VP as Relying Party (Authorized SP attestation)
	c. Must have an EBW for holding Authorized SP attestation (MVP+)
5. EBW provider	a. Must support OpenID4VCI issuance per WBCS cs-01
	b. Must support OpenID4VP presentation per WBCS cs-02
	c. Must pass ITB conformance testing before participating in pilots
6. EBWOID provider	a. As per WP4 requirements

7. Trust registry / Trusted list registrar

a. Must register Issuers of Authorized SP attestations

webuild-consortium / SC5

Q

Type / to search

Code

Issues

Pull requests 1

Agents

Actions

Projects

Security and quality

SC5 / Scenario / Scenario4.md

kjorlaug

Moved pilot participants to scenario description

41ef524 · 3 weeks ago

History

310 lines (223 loc) · 18.1 KB

PreviewCodeBlame

Raw

SC5 — Scenario 4: Direct elnvoicing between Business Wallets

WE BUILD consortium | WP2 — UC SC5

Date	2026-05-24
Version	1.0
Status	Final
Author(s)	Maarten Boender - Sphereon

Part of the SC5 elnvoicing specification suite. Read [Introduction.md](#) for common concepts, roles, attestations and abbreviations.

Index

1. [Introduction](#)

2. [Pre-conditions](#)

3. [Main flow](#)

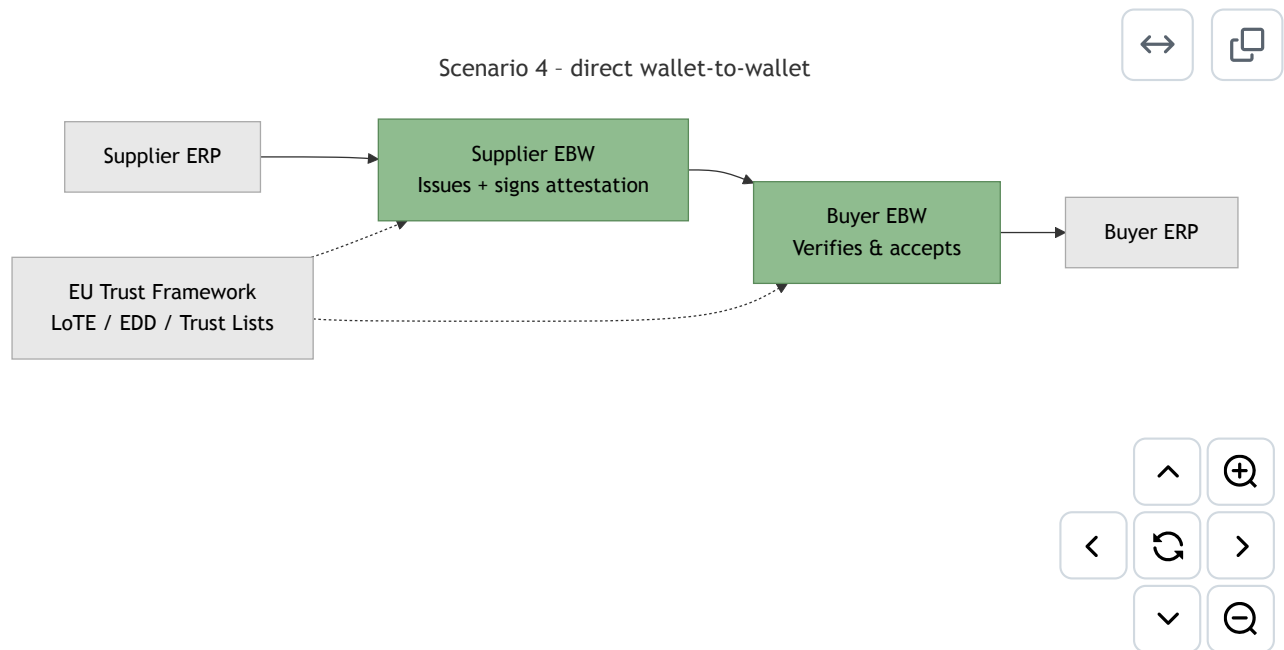
- [3.1 eInvoice preparation and sending by Supplier](#)
- [3.2 eInvoice verification by Buyer](#)
- [3.3 eInvoice with evidence](#)
- 4. [Detailed scenario flow](#)
- 5. [Additional flows](#)
- 6. [Challenges and barriers](#)
- 7. [Working assumptions](#)
 - [7.1 Transfer protocol: OID4VP/DCQL](#)
 - [7.2 \(Q\)ERDS — possible additional pilot track](#)
- [Annex 1 — Requirements for scenario roles](#)
- [Annex 2 — Open issues and decisions log](#)

1. Introduction

Scenario 4 is a cross-border pilot of direct eInvoice exchange where a Supplier issues an eInvoice Attestation and delivers it using their Business Wallet directly to a Buyer Business Wallet, which verifies invoice integrity, supplier identity, and authorization.

Scenario 4 is the only scenario that works independently from the chosen transport layer as it delivers an eInvoice Attestation directly from the Supplier's Business Wallet to the Buyer's Business Wallet in a machine-to-machine context without an intermediary. Trust is not delegated to a network of access points; instead, it is established cryptographically at the point of exchange, through the Supplier's identity binding using the List of Trusted Entities (LoTE) and the integrity of the attestation itself.

This makes Scenario 4 a pilot to test whether wallet-native, peer-to-peer eInvoice exchange, can meet the same integrity and identity assurance requirements as network-intermediated delivery, independent of a shared infrastructure operator in the middle.



The eInvoice Attestation is a verifiable representation (Reference Attestation) of an invoice exchange event, binding invoice content (via a payload hash) to a cryptographic signature associated with the Supplier's legal-person identity. It is used by a Buyer to:

- verify invoice integrity,
- verify the authenticity and validity of referenced evidence (where applicable), and

This scenario is designated **MVP**.

Participants

Role	Organisation	Country
Issuer (Supplier Wallet)	Robert Bosch	DE
Issuer (Supplier Wallet)	Sphereon	NL
Relying Party (Buyer Wallet)	Robert Bosch	DE

The scenario is based on the following documentation:

- WE BUILD SC5 Stock Taking document (V1.0, 11/12/2025)
- ARF / EUDI Wallet specifications (exact version to be confirmed by WP2/4)
- WP2 Semantics outputs for eInvoicing attestations (to be referenced when available)

- Domain standards: EN 16931 (semantic model) and Peppol BIS 3.0 (syntax binding), and ViDA-relevant guidance (where applicable)
- eInvoice Attestation specification ([v0.5 final draft](#))

2. Pre-conditions

- Buyer and Supplier each have an operational Business Wallet instance, capable of issuing, holding and verifying attestations.
- Each wallet instance SHALL be a valid We Build or European Business Wallet bound to a valid Legal Person identity credential/attestation e.g. EU Company Certificate (EUCC) or equivalent.
- Trust anchors are available for verifying legal entity identity binding and signing keys (registry/federation/EDD evidence to be defined by WP4 Trust Registry Infrastructure group).
- The Buyer has a policy decision on inbound acceptance based on a number of checks:
 - Verify signature validity on eInvoice attestation
 - Verify Supplier EUCC/LPID binding (identity valid)
 - Verify Buyer (buyer on invoice = receiving wallet EUCC/LPID)
 - Recompute and verify invoicePayloadHash
- The eInvoice attestation profile (semantics + integrity rules) is agreed and implementable by participating wallet providers.

To establish trust, either the Approved Supplier attestation (as defined in Scenario 1) must be used, or suppliers must be added to a Trust Registry (LoTE/DDE). This decision rests with the WP4 Architecture and/or Trust Registry Infrastructure working groups.

3. Main flow

The flow begins at the Supplier's ERP, which prepares the eInvoice according to the EN16931 semantic model. The payload is canonicalized and an invoicePayloadHash is computed following the agreed rulebook. The ERP submits the payload and associated metadata to the Supplier's European Business Wallet (EBW), which creates and cryptographically signs the eInvoice Attestation.

Before delivery, the Supplier's Wallet resolves the Buyer's Wallet address (a URL endpoint) by consulting the List of Trusted Entities (LoTE), as specified in ETSI TS 119 602. The Supplier's Wallet then presents the eInvoice Attestation directly to the Buyer's Wallet, using the OID4VP/DCQL profile in a machine-to-machine context.

Upon receipt, the Buyer's Wallet performs a sequence of verification steps: it resolves the Supplier's issuer metadata from the Trust Registry and checks the Supplier's authorization status (revocation, expiry, or suspension) against the Status Service. It then verifies the cryptographic signature on the eInvoice Attestation, confirms the Supplier's EUCC/LPID identity binding, verifies that the invoice's buyer field matches the receiving Wallet's identity. Upon receipt of the invoice it recomputes the invoicePayloadHash to confirm the integrity and authenticity of the invoice.

If evidence references are present in the attestation, the Buyer's Wallet retrieves the referenced artefacts from the Evidence Store and verifies their integrity and validity. If no evidence references are present, this step is skipped.

If all checks pass, the Buyer's Wallet clears the invoice and stores the attestation for audit purposes. If any check fails, the invoiceattestation is rejected or quarantined with an error code. In both cases, an optional status message may be returned to the Supplier's Wallet.

4. Detailed scenario flow

Main flow: direct eInvoice exchange between Business Wallets

Invoice preparation (Supplier ERP)

1. The Supplier ERP prepares the eInvoice according to the EN16931 semantic model.

2. The ERP canonicalizes the invoice payload and computes the `invoicePayloadHash` following the agreed rulebook.
3. The ERP submits the invoice payload and associated metadata to the Supplier's European Business Wallet (EBW).

Attestation issuance (Supplier Wallet)

4. The Supplier Wallet creates the eInvoice Attestation, binding the invoice payload hash to the Supplier's legal-person identity.
5. The Supplier Wallet cryptographically signs the eInvoice Attestation.

Discovery and delivery

6. The Supplier Wallet resolves the Buyer's Wallet endpoint (URL) by consulting the List of Trusted Entities (LoTE), as specified in ETSI TS 119 602.
7. The Supplier Wallet presents the eInvoice Attestation directly to the Buyer's Wallet endpoint using the OID4VP/DCQL profile in a machine-to-machine context.

Verification (Buyer Wallet)

8. The Buyer Wallet resolves the Supplier's issuer metadata by querying the Trust Registry.
9. The Buyer Wallet checks the Supplier's authorization status (revocation, expiry, or suspension) against the Status Service.
10. The Buyer Wallet verifies the cryptographic signature on the eInvoice Attestation.
11. The Buyer Wallet verifies the Supplier's EBWOID identity binding.
12. The Buyer Wallet verifies that the buyer field in the invoice matches the receiving Wallet's own identity.
13. The Buyer Wallet recomputes the `invoicePayloadHash` and compares it against the value in the attestation.

Evidence verification (conditional)

14. If evidence references are present in the attestation: the Buyer Wallet retrieves the referenced artefacts from the Evidence Store and verifies their integrity (hash/signature) and validity.
15. If no evidence references are present: this step is skipped.

Acceptance or rejection

16. If all checks pass: the Buyer Wallet **accepts** the invoice attestation and stores it for audit purposes. An optional acceptance notification may be sent to the Supplier Wallet.
17. If any check fails: the Buyer Wallet **rejects or quarantines** the invoice attestation and records an error code. An optional rejection or quarantine notification may be sent to the Supplier Wallet.

5. Additional flows

6. Challenges and barriers

Onboarding or Discovery: how do Supplier and Buyer find each other's Business Wallets?

Answer: The [ETSI TS 119 602](#) specification describes the List of Trusted Entities (LoTE). The EC is proposing the European Digital Directory (EDD) for this. It offers the necessary data and describes the mechanisms for Discovery and Verification. There is an [ADR](#) proposed for this.

For now the transport protocol will be OID4VP & DCQL. Depending on the upcoming Implementing Acts we may also need to pilot another transport protocol (QERDS?).

Clarity of role:

- Supplier issues eInvoice attestation
- Buyer holds eInvoice attestation
- Buyer Business Wallet technically verifies the Invoice attestation and Accepts (or not)
 - Integrity
 - Trust establishment
 - Third party may verify and accept eInvoice attestation (e.g. software provider checks integrity rules)
 - eInvoice xml integrity validation

- Note: buyer is equipped to further process the elnvoice information / paves way for automation (out of scope)

7. Working assumptions

7.1 Transfer protocol: OID4VP/DCQL

Transfer protocol: OID4VP/DCQL (pilot choice) in a Machine 2 Machine context

OID4VP/DCQL is primarily about the semantics and security of verifiable presentations: what the Relying Party asks for (constraints), how the holder proves it (presentation), and how replay and audience binding are handled (nonce/audience/state). It does not require that the Relying Party (buyer) "starts the business process"; it requires that the Relying Party (buyer) controls the request object (or at least the parameters that make the response verifiable and non-replayable).

In our pilot, the Supplier initiates sending because it already has the Buyer's contact data (wallet address + API endpoint). That can still fit OID4VP/DCQL if we implement a short handshake where the Supplier fetches the Buyer's request object before submitting the presentation.

A workable supplier-initiated flow looks like this:

- Supplier wallet already has Buyer Relying Party endpoint (from contact data).
- Supplier wallet calls Buyer endpoint to obtain a fresh Presentation Request (OID4VP Request Object) that contains:
 - DCQL query constraints (what Buyer will accept),
 - nonce + audience + expiry window,
 - state/correlation identifier and the submission endpoint.
- Supplier wallet submits the invoice package as an OID4VP response (presentation) to the Buyer endpoint:
 - elnvoice Attestation,
 - invoice payload (or reference),
 - optional evidence references (or included evidence).
- Buyer verifies:
 - the presentation response integrity (signature/holder binding as defined),

- the supplier's legal-person identity binding (EUCC/LPID or equivalent),
- invoice payload hash binding and any evidence integrity/validity checks.

This is "Supplier-initiated delivery" operationally, while keeping "Relying Party-defined requirements" cryptographically and semantically.

7.2 (Q)ERDS — possible additional pilot track

It may be that the upcoming Implementing Acts defined by the European Commission may require use of the (Q)ERDS protocol for exchange of data.

ERDS/QERDS is about the delivery channel and the evidentiary value of sending/receiving, not about "what claims are requested" in the same way.

Conceptually:

- ERDS provides registered electronic delivery evidence (proof of sending and proof of receipt/delivery) with integrity protection.
- QERDS is the qualified eIDAS variant, delivered as a qualified trust service, with stronger and more harmonised legal effects for the evidence.

In eInvoicing, we should use ERDS/QERDS when the delivery evidence itself must be strong and dispute-proof ("who sent what to whom and when"), potentially because the Commission's upcoming Business Wallet implementing decisions may require (qualified) registered delivery capabilities for certain exchanges.

These are not mutually exclusive with OID4VP/DCQL. Two common positions are:

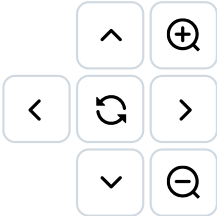
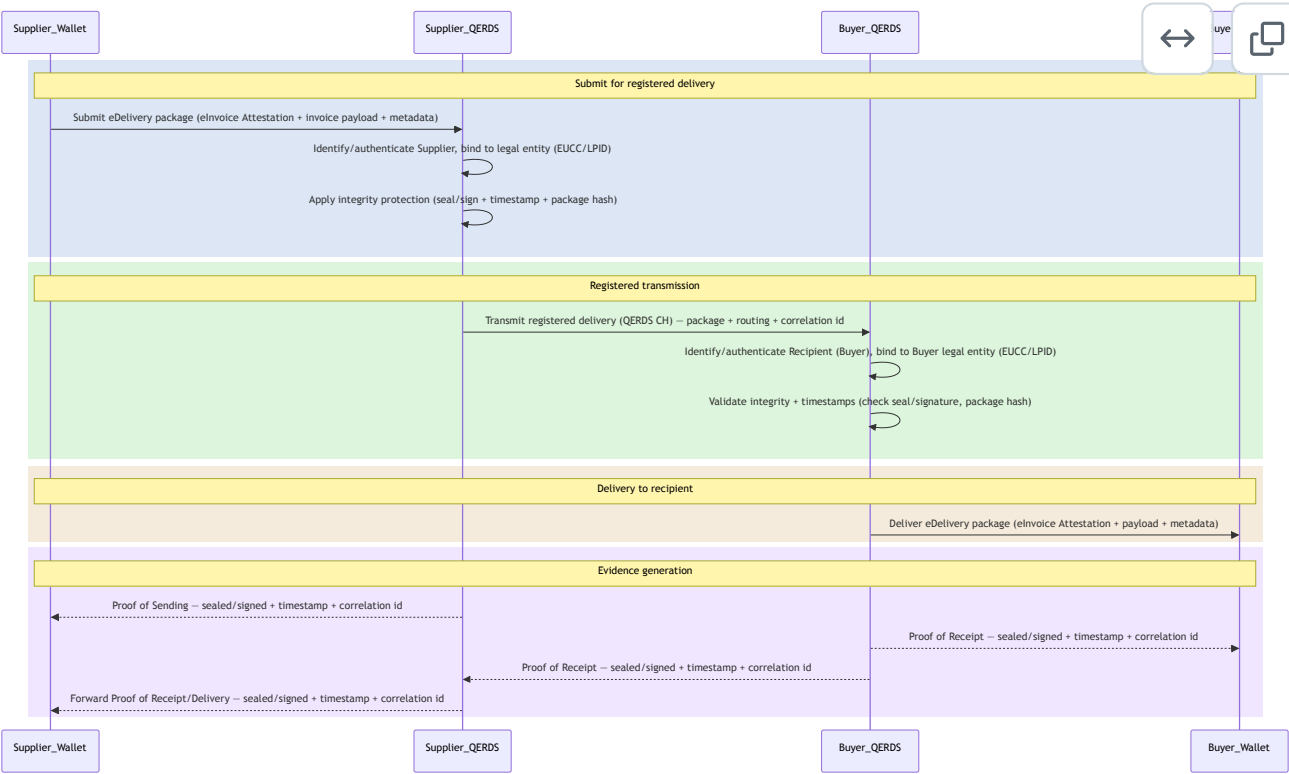
- Choose OID4VP/DCQL when you primarily need interoperable wallet/presentation semantics (constraints, selective disclosure, consistent verification), and you can rely on ordinary HTTPS/API transport plus application logs for delivery evidence.
- Add ERDS/QERDS when you also need legally stronger delivery evidence. ERDS/QERDS can wrap the same payload (eInvoice Attestation + invoice data) as the delivery channel, while OID4VP/DCQL governs the internal presentation semantics.

Decision guidance

Decision factor	OID4VP/DCQL	ERDS	QERDS

Primary purpose	Interoperable presentation semantics and Relying Party constraints	Registered delivery evidence (non-qualified)	Highest-assurance registered delivery evidence (qualified)
Who initiates operationally	Buyer provides request object. Supplier initiates.	Supplier initiates; delivery service transports	Supplier initiates; qualified delivery service transports
What you can prove best	The buyer received a verifiable presentation that satisfies buyer-defined constraints	Sent/received with integrity and evidence of delivery	Same as ERDS, but with qualified evidentiary strength
Dispute profile	Normal (as is today)	Elevated risk of dispute	High-value / High-risk / Regulated
Dependency on buyer endpoint	Yes (needs request object and submission endpoint)	Less strict (delivery channel can queue/retry)	Less strict (delivery channel can queue/retry)
Operational complexity	Low	Medium	Highest (qualified trust service onboarding/ops)
If implementing acts push registered delivery	Might still be needed for presentation semantics, but transport may need ERDS/QRDS	Possible	Likely if "qualified" is required

The following diagram illustrates the (Q)ERDS direct send/receive flow:



Annex 1 — Requirements for scenario roles

 *To be completed during specification phase based on partner input.*

Primary role	Specific requirement
User of Business Wallet	
Authentic sources	
Relying party	

Intermediary	
Business Wallet provider	
PID Provider	
Trusted list registrar	
QEAA provider	
Pub-EAA provider	
EAA provider	
QES provider	

Annex 2 — Open issues and decisions log

#	Issue	Status	Responsible
1	Decide invoice payload canonicalization method(s) and hash strategy.	open	WP4 Architecture
2	Decide invoice semantic (e.g. EN16931 semantic model, Peppol BIS 3.0 UBL syntax, or both with one as primary) or align to ViDA.	open	WP4 Semantic
3	Decide trust anchor mechanism for LPID and signing keys (LoTE/DDE registry vs federation vs QTSP signals).	open	WP4 Trust Registry
4	Decide minimum disclosed invoice elements for validation vs privacy.	open	