

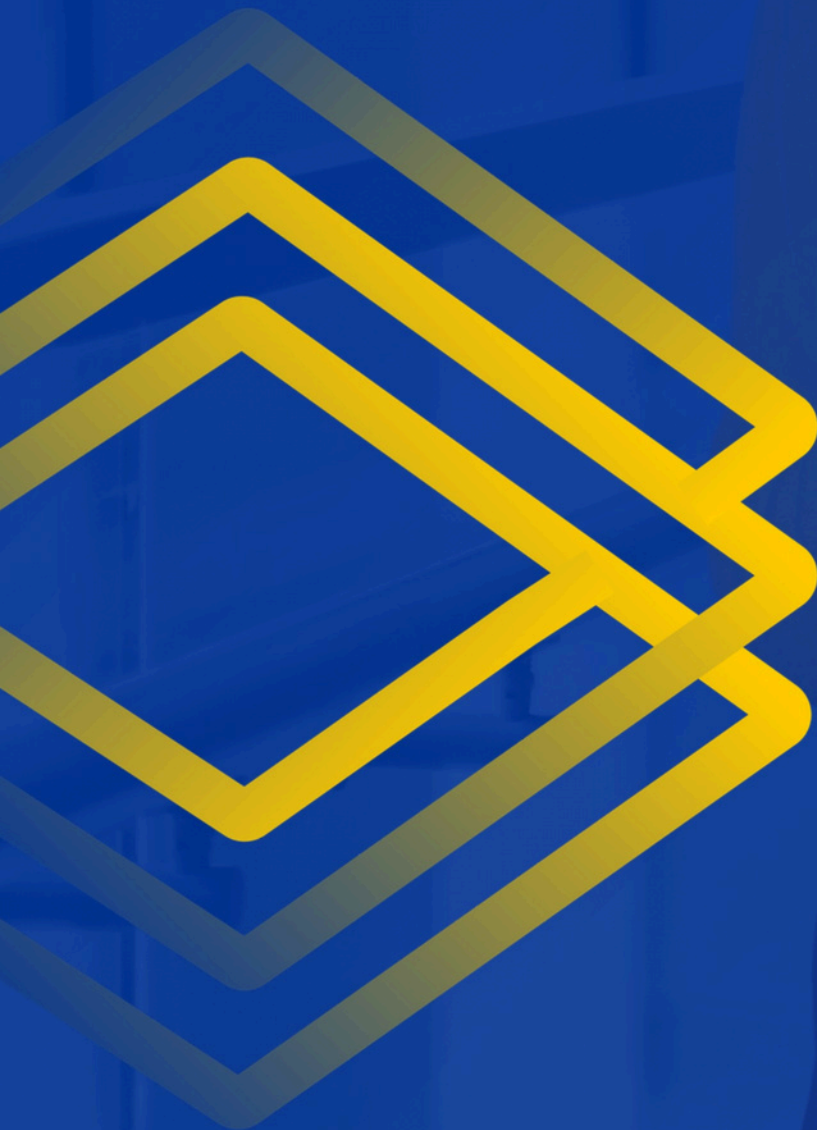


WE BUILD
CONSORTIUM

Deliverable D3.1

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 payments U se cases on I dentification, L egal representation and D ata sharing
Grant Agreement no	Project 101224751 — WE BUILD
Deliverable title	D3.1 Pilot Design
Deliverable type	R – Document, report
Responsible party	Stichting ICTU
Authors	Marie Austenaa, Ard van der Heijden
Contributing parties	Mastercard Europe, Stichting ICTU
Reviewers	Marie-José Hoefmans, Frans de Kok, Arno Fiedler, Maria Cristina Timon Lopez, Arthur van der Wees, Dimitra Stefanatou, Franziska Granc, Joost Fleuren, Stef Haartman, Bob Kronenburg, Rob Brand, Paloma Llana, Giulia Messori
Dissemination level	Public

History of changes

Version	Date	Change
0.1	3 June 2026	Setup template and ToC
0.2	22 June 2026	Initial production of sections
0.6	3 July 2026	First draft for review
0.7	9 July 2026	Included CH 4
0.8	13 July 2026	Second draft for review
0.89	22 July 2026	Internal processing of review completed
0.9	24 July 2026	Ready for approval
1.0	30 July 2026	Approved for submission

Table of contents

Table of contents	3
1. Executive summary	6
2. Introduction	7
2.1 Scope and goal	7
2.2 Target audience.....	7
2.3 Versioning.....	7
3. Approach of the pilot design.....	8
3.1 Introduction.....	8
3.2 Phased approach.....	8
3.3 Prioritization	9
3.4 Deliverables and templates	9
3.5 Dependencies	10
3.6 Roles and responsibilities.....	11
3.7 Evaluation strategy.....	12
3.8 Collaboration with other work packages.....	12
3.9 Collaboration with APTITUDE	12
4. Overview of use cases	13
4.1 Regulatory considerations	14
4.2 Payments domain use cases	17
4.2.1 Use case PA1 – consumer bank account opening.....	17
4.2.2 Use case PA2 – Consumer payments.....	21
4.2.3 Use case PA3 – Business bank account opening.....	25
4.2.4 Use case PA4 – Business payments	27
5. Scoping decisions and working assumptions	30
5.1 Scoping decisions.....	30
5.2 Main working assumptions	31
6. Expected learnings	35
6.1 Integration of wallet trust into existing sector systems	35
6.2 Attestation usage across processes	35
6.3 Wallet Dance	35
6.4 User Experience.....	36
6.5 Attestation Standardization.....	36
7. Challenges and risks	37
7.1 Introduction.....	37
7.2 Main challenges.....	37
7.3 Main risks	38

8. Conclusion.....	41
Annex A – Use case / attestation matrix MVP/MVP+	42
Annex B – Use case / country matrix	43
Annex C – MVP scenario specification documents	44

List of figures

Figure 1: Phased approach of the work-package.....	8
Figure 2: Overview of WP3	11

List of tables

Table 1: PA1 Scenario 1	19
Table 2: PA1 Scenario 3	20
Table 3: PA1 Scenario 4	20
Table 4: PA1 Scenario 5	21
Table 5: PA2 Scenario A1	23
Table 6: PA2 Scenario A2	23
Table 7: PA2 Scenario B1	24
Table 8: PA2 Scenario B2	25
Table 9: PA3 Scenario 1	26
Table 10: PA3 Scenario 2	26
Table 11: PA3 Scenario 3	27
Table 12: PA4 Scenario 1.1	28
Table 13: PA4 Scenario 1.2	29

Abbreviation	Meaning
A2A	Account-to-account (payment)
ARF	Architecture Reference Framework
BU1	Business use case 1 (work package 2)
DC API	Digital Credentials API (browser-wallet and OS-wallet integration)
DC4EU	Digital Credentials for Europe (Large Scale Pilot)
EBW	European Business Wallet
EBWID	European Business Wallet Organisation Identifier
EUDI Wallet	European Digital Identity Wallet
EU PoA	European Power of Attorney attestation
EUCC	European Company Certificate
HADEA	European Health and Digital Executive Agency
IBAN	International Bank Account Number
KYC	Know Your Customer
LSP	Large Scale Pilot
mdoc	Mobile document (ISO 18013-5 style credential format)
NOBID	Nordic-Baltic eID project (Large Scale Pilot)
PID	Person Identification Data (wallet identity credential)
PSD2	Payment Services Directive 2
PSR	Payment Services Regulation
QTSP	Qualified Trust Service Provider
QES	Qualified Electronic Signature
SCA	Strong Customer Authentication
SCA Card	SCA for card payments
SCA-IBAN	SCA attestation bound to an IBAN
SCA-User	SCA attestation bound to a user
SD-JWT	Selective Disclosure JSON Web Token
TS12	Technical Specification 12 (payments-related spec) in the ARF
UBO	Ultimate Beneficial Owner
VAT ID	Value Added Tax Identifier
VC	Verifiable Credential
WP2	Work Package 2 (business and supply chain)
WP3	Work Package 3 (payments and banking pilots)
WP4	Work Package 4 (architecture and technology)
WP5	Work Package 5 (business case, governance, MSAB)
WP6	Work Package 6 (communication and dissemination)
WE BUILD	Wallet Ecosystem for Business and Payments Use cases on Identification, Legal representation and Data sharing

1. Executive summary

This deliverable presents the pilot designs for the Payments use cases that will be executed in Work Package 3 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 use cases cover 13 high-prioritized scenarios, exercising 24 different types of attestations to be used in settings for bank account opening and payments by citizens and companies. An additional 7 lower prioritized scenarios have been detailed as well, which are positioned as ‘stretch-goals’ for the use cases. All scenarios stayed close to the 6 key-objectives in the WE BUILD project.

The high prioritized use cases target typical scenarios like opening a bank account and issuing a Strong Customer Attestation for later Identity Matching use, issuance and use of IBAN attestations for account-to-account payments, doing online card payments, extending general KYC-process with additional attestations needed for account-opening for businesses and doing payments of eInvoices. Especially in the payments use case for natural persons much attention existed for the UX-aspect of the process. Although this will not be piloted, research will be done to the role of AI-agents in the payment processes.

This document provides a high-level description of the high-priority scenarios for each use case. More detailed and highly focused designs, including process flows, assumptions, attestation rulebooks and country mappings, are provided in annexes to keep the main deliverable accessible while still supporting implementation teams with sufficient detail.

The designs build explicitly on the results of previous Large-Scale Pilots (POTENTIAL, NOBID, EWC, DC4EU). Existing attestation designs and solutions were reused where possible and then refined to address new challenges, extend coverage and create additional value in the WE BUILD context.

Cross use case alignment structures were installed in the work-package to ensure coherence and increase the adoption of solutions that were designed. Also a Financial Interest Group was created to inform interested people and companies outside of WE BUILD, about what WE BUILD is piloting.

Piloting faces several key challenges and risks. These include evolving standards and regulations that may impact the designs, the need to involve the right partners in sufficient numbers, and the balance between the remaining workload and the available time in the project. To address these, the work package applies stricter change management, continuous recruitment and engagement of partners, close monitoring of progress, and strong prioritisation to safeguard delivery of the core elements of each use case.

2. Introduction

2.1 Scope and goal

This document is the first formal deliverable of Work Package 3 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 and 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, banking, finance 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 PAYMENT and BANKING 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 pilot design

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 4 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.

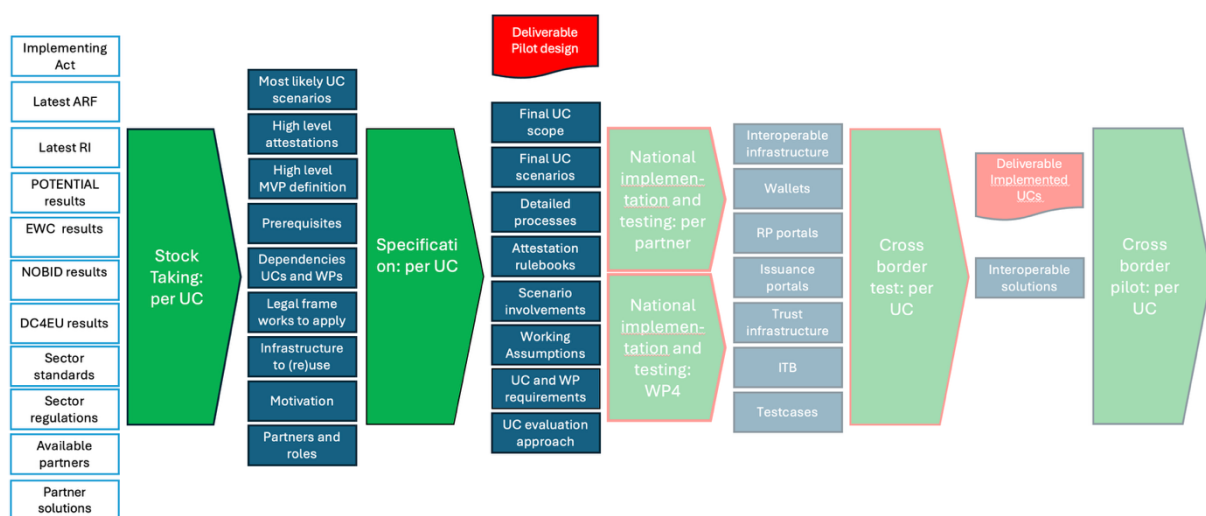


Figure 1: Phased approach of the work-package

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 thirteen use cases into more concrete 'pilot definitions'. It identified nineteen scenarios in total, of which twelve were classified as high priority using twenty-four 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 begun 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. In WP3 this was not the case and only SD-JWT is used. For use cases progressing quickly, working with alternative formats will be considered later in the project, if necessary.

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:

- 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 D3.1 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 cannot 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 solutions 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 mostly 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 roughly 40 attestations and over 20 involved countries, maintaining these mappings was an intense but necessary effort.

3.6 Roles and responsibilities

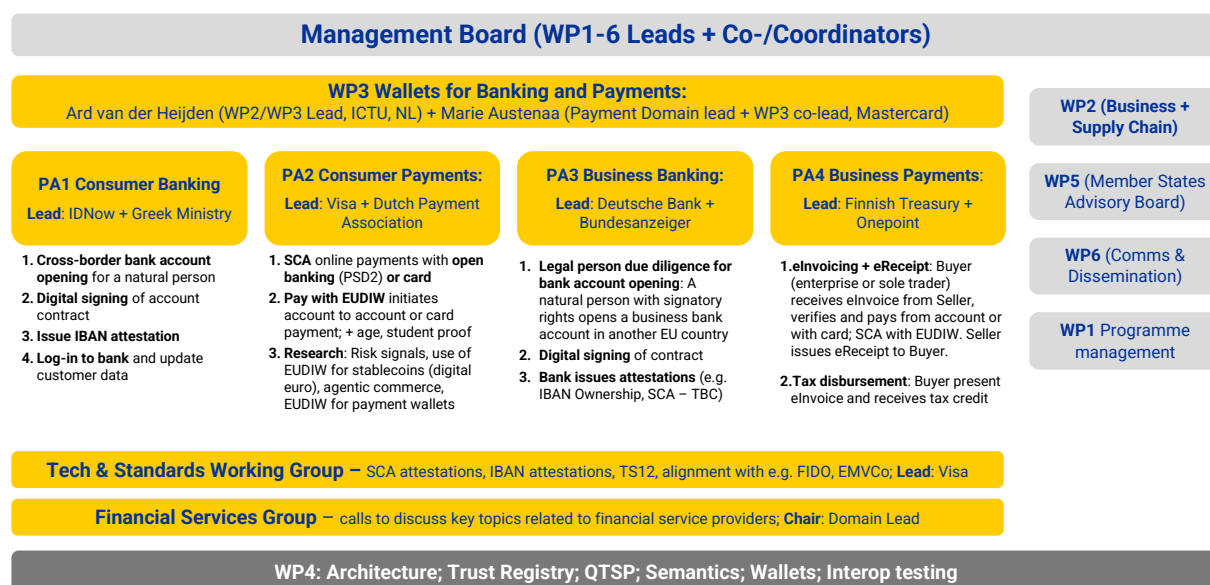


Figure 2: Overview of WP3

Use case leads and co-leads carried primary ownership and drive 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 formal 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.

WP3 addressed certain challenges common to the use cases, in separate groups:

- A ‘Technology & Standards group’ (T&S) was established, consisting of technical representatives of all payment use cases. The group addressed topics like TS12, IBAN attestations design, Strong Customer Authentication etc to secure uniform application of these topics across all payment use cases.
- A ‘Financial Services Group’ internal to WE BUILD was created, allowing additional alignment on topics of importance for banks, even if a bank was not involved in every payment related use case. Payment services regulation for the use of the EUDI wallet for strong customer authentication was one of the key topics discussed. This way, a stronger foundation can be created for industry adoption and roll-out after the LSP.

- A ‘Payment Interest Group’ was established, allowing also non-WE BUILD organizations to stay informed about the developments in WE BUILD. The first meeting interested over 130 persons and was held in June 2026. Also here, the aim is to increase the strength of adoption of the EU DI and Business wallets for payments.

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 (digital wallet providers, PID/EBWOID providers, QTSPs, semantics group, etc.). For WP3 this was concentrated in 1 person, that was also the lead of the T&S group. This way, the T&S group could stay aligned with the generic WP4 architecture workgroup.

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 WP3 and WP4 to secure feasibility of the scenario as well as increase 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. WP3 and WP5 co-worked together to establish the Payment Interest Group.

3.9 Collaboration with APTITUDE

WE BUILD and APTITUDE have agreed on sharing experiences and designs across LSPs and expressed the interest in a potential cross-LSP-pilot, provided the right circumstances. To maintain alignment, a monthly meeting was held where ideas, progress, challenges and design-decisions were discussed. Based on that, WE BUILD and APTITUDE brought shared views and challenges to the European Commission during regular meetings.

At some point, APTITUDE had to pause the work package addressing payment use cases. This did not impact WE BUILD, but alignment on payment related topics did see a temporary reduction in effectiveness. The idea of a cross-LSP-pilot is still on the table and will be evaluated on a regular basis.

4. Overview of use cases

This chapter describes the use cases existing in Work Package 3, targeting the payments and banking domain. Each use case will be described on a high level, explaining the core of the use case. In addition, 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.

EU DI Wallet (EUDIW) and EU Business Wallet (EUBW) can reduce fraud, simplify payment and banking services, drive innovation and new services, support the industry to satisfy regulatory obligations – and **make it easier to leverage the scale of EU for financial services**, i.e.:

- **Know-your-Supplier (KYS)** easy to onboard SMBs – bring new business opportunities
- **B2G - simplify processes for businesses to interact with governments**
- **KYB and KYC for cross-border account** opening simplify expansion into other markets
- **Seamless user experience, reduced fraud and regulatory compliance** in payments

The use of the EUDI and Business wallets in banking and payment can **create the virtual cycle needed to drive adoption** of the EU wallets by making them useful for everyday use

eIDAS obligations requires financial service providers to use the EUDIW for ID verification, online log-in, risky actions such as confirming changes to account or setting up a new direct debit, and frequent transactions such as payment authentication (PSD2/PSR SCA). Similarly, the proposed EUBW regulation obliges public sector to use the digital wallet. This can encourage adoption.

If there is broad adoption of the EU wallets, businesses and governments can design seamless and secure services, further driving adoption – creating a **positive feedback loop**.

However, payments and banking services relies on industry specific regulation, well established standards and extensive legacy infrastructure with high requirements for resilience, resistance to fraud, and high expectations of a seamless and fast user experience.

The use case pilots that we are preparing for in WE BUILD needs to accommodate these requirements and balance this against the developing eIDAS implementing acts and evolving global standards. Our objective is to seek solutions that are practical and have the potential to scale by involving stakeholders across the complex payment eco-system.

The purpose of this chapter is to present the scope of payment and banking pilots in WE BUILD and the learnings we seek from these pilots.

A note on attestations:

To deliver the pilot, we rely on the ARF TS12 for initial technical solution. This means that we will issue and verify attestations which are specific to authentication flows – “SCA Attestation”. These attestations are issued by the bank (or an intermediary) and verified either by a third party or by the issuer. These attestations come in different flavours: SCA-Card

- SCA-User
- SCA-IBAN
- IBAN Ownership

Other attestations that we will use are: eReceipt, Student Status, Tax ID, VAT ID. These are use case specific, and will be introduced in the section for the relevant use case.

4.1 Regulatory considerations

WE BUILD assumes the EUDIW will be used for SCA and explores the related technical and regulatory implications. This content is not legal advice and does not necessarily reflect the views of all WE BUILD participants.

The Legal Anchor: eIDAS 2 Article 5f(2)

The regulatory foundation for using the European Digital Identity Wallet (EUDIW) in payments and banking is anchored in [Article 5f\(2\) of the eIDAS 2 Regulation](#). The provision states that where private relying parties — including in the fields of banking and financial services — are required by Union or national law to use strong user authentication, they shall, upon the voluntary request of the user, also accept European Digital Identity Wallets. This creates a direct legal bridge between eIDAS 2 and PSD2's Strong Customer Authentication (SCA) obligation: the digital EUDI wallet becomes a valid means for satisfying SCA whenever the user chooses to use it, and payment service providers are obliged to accept it.

Interpretive Guidance from the European Commission

Recognising the ambiguity that inevitably arises when two major regulatory frameworks intersect, [DG CONNECT and DG FISMA have jointly published a Q&A on eIDAS and SCA](#). While not legally binding in the strict sense, it provides authoritative directional guidance to the industry and clarifies four points that are essential for the design of digital wallet-based SCA:

- **SUA and SCA are equivalent for the purposes of PSD2 SCA.** The Strong User Authentication concept introduced by eIDAS 2 satisfies the Strong Customer Authentication requirement of PSD2. There is no separate authentication standard to satisfy.
- **Banks are obliged to accept the EUDIW.** The Q&A confirms the reading of Article 5f(2) that payment service providers must accept the digital EUDI wallet when the user chooses to use it.
- **The Q&A explains how the EUDIW is to be used to fulfil PSD2 SCA obligations**, with explicit reference to **TS12** — the technical specification annexed to the ARF that details how SCA is implemented with the digital EUDI wallet.
- **Use of the EUDIW for SCA does not imply that SCA is delegated.** Because SCA is not delegated, there is no need for outsourcing agreements between payment service providers and digital EUDI wallet providers, removing what would otherwise be a very significant contractual and operational barrier to adoption.

Reinforcement in the PSR Consolidated Draft (18 May 2026)

The same direction is reinforced in the **consolidated draft of the Payment Services Regulation (PSR) of 18 May 2026** — the Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010:

- **Recital 111** explicitly recognises “European Digital Identity Wallets (...) as electronic identification means offering identification and authentication tools for accessing financial services across borders, including payment services.” It confirms that, “pursuant to Article 5f(2) of Regulation (EU) No 910/2014, **payment service providers will be under an obligation to accept the use of the EU Digital Identity Wallets for supporting the fulfilment of SCA requirements** for online identification for account login and for the initiation of payment transactions”. The recital also tasks the **EBA with drafting regulatory technical standards** that specifically take into account the use of the EUDIW to support the fulfilment of SCA requirements for these purposes.
- **Article 89(3)** provides that, in accordance with Article 10 of Regulation (EU) No 1093/2010, the EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis to take account of innovation and technological developments, the provisions of Chapter II of Regulation (EU) 2022/2554 (DORA), and the European Digital Identity Wallets implemented under Regulation (EU) No 910/2014.

The combined effect is that the obligation to accept the EUDIW for SCA is explicitly restated in the payments-specific regulatory framework, with the EBA formally tasked to translate this into RTS.

WE BUILD Perspectives (Not Legal Opinion)

Given this landscape, the consortium has adopted a pragmatic position to enable pilots to move forward without waiting for every regulatory detail to be finalised:

- **Direction:** Move forward with digital EUDI wallet-based SCA as the working assumption for pilot design.
- **Pilot philosophy:** Proceed with workable assumptions, validate in practice, and refine later as regulatory clarity emerges and pilot findings accumulate.

Within this philosophy, three regulatory topics are treated as central to pilot design:

1. Roles and responsibilities of the digital wallet vs. the PSP

The EUDI wallet must not perform any function that could be interpreted as taking over the authentication of the payment transaction itself. Responsibility for authenticating the payment transaction remains with the PSP; the EUDI wallet acts as an authentication *tool* invoked by, and answerable to, the PSP. This distinction is what keeps SCA from being considered "delegated" and therefore preserves the no-outsourcing outcome confirmed by the Commission Q&A.

2. PSP ability to demonstrate control over the ecosystem in the context of the EUDI wallet

For PSPs to remain accountable under PSD2 and the PSR, they must be able to demonstrate operational control over the authentication ecosystem, including when that ecosystem includes third-party digital wallets. Three mechanisms are being explored in WE BUILD:

- **Certification** — EUDI wallets must be certified, and the scope of certification must reflect the technology and processes actually used to perform SCA. This is a prerequisite for PSPs to rely on the digital wallet with confidence.
- **Risk signals** — EUDI wallets must generate risk signals so that the PSP can detect risks and abnormalities. This is directly linked to the PSR's provisions on transaction monitoring (notably Article 83 of the PSR draft).
- **Integrity and assurance indicators** — EUDI wallets must share integrity and assurance indicators so that the PSP can determine whether EUDI wallet-related controls have been compromised. Further work is needed to identify which risk and assurance signals PSPs actually require, and which of these can realistically be supported by EUDI wallet ecosystems as they are being deployed by Member States.

3. Allocation of liability between PSP and EUDI wallet, linked to control and influence

Liability allocation should follow the principle that responsibility tracks control. Each step of the flow — registration/issuance of the SCA attestation, presentation of the credential, verification, and hold — should be evaluated to determine which entity (PSP, digital wallet provider, or PID issuer) has influence over the actions and which party can detect issues or anomalies. Liability should then be aligned with that level of control and visibility. This is an area of active work and will require input from regulators, EBA RTS, and pilot evidence before a stable model can be codified.

Other Regulatory Topics we will investigate during the pilot

Beyond the core SCA question, the consortium continues to monitor and work on a number of adjacent regulatory topics that will shape adoption at scale:

- **Certification of digital wallets** — including the scope of certification required to support payment SCA and the interaction between national certification schemes and the future ENISA-run pan-European scheme.
- **Development of TS 12** — as the technical anchor for digital wallet-based SCA, its evolution and potential inclusion in an implementing act will be decisive for industry investment.
- **Risk and fraud signals** — defining the minimum set of signals that digital wallets should expose to PSPs to preserve fraud detection capabilities.
- **Regulatory clarity through EBA RTS for PSR** — the EBA's forthcoming regulatory technical standards will translate the high-level obligations of the PSR into operational requirements, and industry engagement in that process is essential.

The regulatory direction of travel is now sufficiently clear for the industry to design and pilot EUDI wallet-based SCA with confidence: eIDAS 2 Article 5f(2), the Commission's Q&A, and the PSR consolidated draft all converge on the same conclusion — banks and payment service providers must accept the EUDIW for SCA, the EUDI wallet does not constitute delegation, and no outsourcing agreement is required. What remains to be settled is the detail: certification

scope, standardisation of attestations, risk and assurance signals, EBA RTS under the PSR, and liability allocation. WE BUILD's pilots strive to produce concrete evidence on these open points.

Strong Customer Authentication

Strong customer authentication is implemented in accordance with ARF TS12:

- [ARF §2.6.4 — Strong User Authentication for Electronic Payments](#)
- [ARF — TS12 Specification of Strong Customer Authentication \(SCA\) Implementation with the Digital wallet](#)

Strong User Authentication comprises the following phases

- **Registration:** The User registers the Digital wallet Unit as an authenticator for a service. This process includes:
 - User identification and authentication, for example by presenting a PID,
 - User consent for the registration,
 - Linking a Wallet Unit with the service and a User account in that service. This happens by issuing a dedicated SUA attestation to the Wallet Unit, containing User attributes relevant for the service. The issuance process for this SUA attestation complies with all requirements for attestation issuance in this ARF. The SUA attestation is device-bound, which means it contains a public key, and the associated private key is stored in a WSCA/WSCD or in a keystore.
- **Strong User Authentication:** A Relying Party sends a presentation request to the Wallet Unit to request relevant attributes from the SUA attestation. This presentation request includes transactional data. In the context of electronic payments, the transactional data will include at least the payment amount and the payee. After presenting the data to the User and obtaining the User's approval, the Wallet Unit signs the transactional data. It does so by including (a representation of) the transactional data in the signature creation process used for device binding. Note that the syntax and semantics of the transactional data, as well as rules for how the data must be presented to the User and how the data will be prepared for inclusion in the device binding signature, will be defined in the Attestation Rulebook (or a Technical Specification) for the SUA attestation.
- **De-registration:** Unlinking the Wallet Unit from the service and/or the User's account in that service. This will involve deletion or revocation of the SUA attestation.

4.2 Payments domain use cases

4.2.1 Use case PA1 – consumer bank account opening

The purpose of this use case is to demonstrate use of EUDIW for cross-border opening of a personal bank account in compliance with AML Regulation. We seek to demonstrate secure and seamless verification of natural person identities and explore the implications and benefits of using an intermediary to facilitate. Upon identity verification, the consumer signs a contract for account opening, and the bank issues an IBAN attestation as proof of IBAN ownership into the EU DI wallet as well as an SCA-User attestation to enable the account holder to log back into the online bank. The IBAN attestation will enable the digital wallet for pay by bank in later use cases. This use case includes the following scenarios; each elaborated in further details below:

1. Cross-border bank account opening
2. Digital signing of account contract
3. Issue IBAN and SCA-User attestations
4. Log-in to bank and update customer data

Questions to explore:

- **Regulatory & Compliance:** Compliance with AMLR? Are there authentic sources for all attestations? Do QTSP-issued attestations work as a credible interim — and where should the root of trust ultimately sit?
- **Intermediaries:** What is the role and benefits of intermediaries? What are the technical implications? How can the expected regulatory position be implemented? Are there gaps in regulation or technology? How does the use of intermediaries affect bank efforts? How does the role of an intermediary affect the UX?
- **User experience:** How to optimise user experience? How do we optimise UX across same-device and cross-device flows, including the trade-off between the DC API and its Custom URI / deep-link fallback?
- **IBAN & attestation value:** Which data are required for an IBAN attestation and how to ensure there is an industry standard? What is the value (fraud reduction, reuse across banks) to the industry of IBAN attestations? How to manage the issuance/renewal/revocation lifecycle?
- **Ecosystem readiness:** Is the trust infrastructure (Trusted Lists, Access/Registration Certificates, status/revocation) and cross-wallet, cross-border interoperability mature enough to pilot reliably? What are requirements and possible barriers to scaling?

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	Cross-border bank account opening
Description	A natural person opens a personal bank account cross-border (a resident of Country A opening an account in Country B) or in-country, using the EUDI Wallet to securely provide identity and KYC data to the bank in line with the Anti-Money Laundering Regulation (EU) 2024/1624. The bank integrates (directly or via an intermediary) with the EUDI wallet to request a PID and the other required attestations via OpenID4VP, validates them against the WE BUILD trust infrastructure and, upon successful KYC, presents the terms and conditions for the consumer to sign, and concludes the account opening. The scenario targets low/medium-risk clients that have chosen to hold an EUDIW. If the bank has selected to integrate with the EUDIW through an intermediary, then this intermediary platform manage all EUDIW and trust infrastructure interactions on behalf of the bank. The intermediary holds its own Wallet Relying Party Access Certificate, registers the

	intermediated bank in the Member State Registrar, verifies the presented PID and (Q)EAAs (issuer signature and trust chain, revocation status, holder binding), validates them against the attestation rulebooks, normalises the data into a common API response and forwards it to the bank only after successful checks, without persisting any personal data. This minimises the bank's integration effort.
Setting	Remote onboarding via the bank's website or app; both same-device (deep link) and cross-device (QR code) flows are piloted, with the W3C Digital Credentials API (DC API) as an optional invocation mechanism. If an intermediary platform is used, then the wallet displays both the intermediary and the bank to the user during consent (e.g. 'Requestor: [Intermediary] on behalf of: [RP]').
Wallet types used	EUDI Wallet (EUDIW) for natural persons. No Business Wallet (EBW) for bank to support mutual authentication is planned for
Attestations used	Consumed: PID (provided by WP4/PID providers; the attributes 'portrait' and 'personal_administrative_number' must be populated). Issued: TaxID, Certificate of Residence and IBAN Ownership. As no authentic sources were identified, TaxID and Certificate of Residence are issued as mock (Q)EAAs by the PA1 QTSPs (e.g. IDnow, InfoCert). The IBAN Ownership attestation is issued by the relying-party bank in PA1.
Countries involved	Relying party countries: CZ, GR, IT, NL, RO. PID issuing countries: CZ, DE, ES, IT.
Number of relying parties	7 banks (Air Bank, ČSOB and Komerční Banka (CZ), National Bank of Greece (GR), Banca Sella (IT), ABN AMRO (NL) and Banca Transilvania (RO). Served via up to 6 intermediaries: Authologic, itsme, Mastercard, Walt.id, Lissi and Bank ID.

Table 1: PA1 Scenario 1

Name	Sign contract
Description	Cross-border signing of legally binding bank contracts by natural persons with a Qualified Electronic Signature (QES) via the EUDI Wallet, with legal equivalence to handwritten signatures across the EU (eIDAS 2.0). The MVP covers signing of the account-opening contract during onboarding using the QTSP-centric model, in which the digital wallet authenticates and authorises a remote signing service and the QES is created on a remote QSCD operated by IDnow Trust Services AB. The digital wallet applies the 'what you see is what you sign' principle: it renders the contract and the transaction data and recomputes the document hash before the user authorises the QES. Wallet-centric signing (local QSCD) and subsequent service contracts are MVP+.
Setting	Remote signing from the bank portal after login with the SCA-User attestation (issued in PA1 Scenario 4); same-device deep link and cross-device QR flows via OpenID4VP 1.0; hash-signing as the primary integration pattern (full PDF signing optional).
Wallet types used	EUDI Wallet for natural persons only; EU Business Wallet and Company Representative flows are out of scope for PA1.

Attestations used	Consumed: PID and SCA-User (from PA1 Scenario 4). Issued: a short-term QES certificate bound to the natural person and the QES applied to the contract, both issued/created by IDnow Trust Services AB (SE) and verifiable cross-border via the EU trust lists.
Countries involved	Relying party countries: GR, IT. PID issuing countries: CZ, GR, IT. QES issued from SE.
Number of relying parties	2 banks: National Bank of Greece (GR) and (optional) Banca Sella (IT).

Table 2: PA1 Scenario 3

Name	Attestation issuance (SCA, IBAN)
Description	Issuance of banking attestations to the EUDI Wallet of an onboarded customer: SCA-User (authentication to the bank and confirmation of actions requiring strong authentication), SCA-IBAN (as SCA-User, plus PISP payment initiation) and IBAN Ownership (confirmation of account ownership/control). The bank acts as authentic source and may delegate the digital wallet-facing issuance to a dedicated EAA issuer. Issuance follows OpenID4VCI (HAIP profile per the WP4 architecture) and the SCA attestation designs of ARF Technical Specification 12; the issued attestations are consumed in PA1 Scenarios 2 and 3 and in the PA2 payment scenarios.
Setting	Remote issuance from the bank's website or app (credential offer via QR code, deep link or DC API), either as a direct continuation of onboarding (Scenarios 1 and 2) or initiated by an existing bank customer.
Wallet types used	EUDI Wallet for natural persons.
Attestations used	Consumed: PID (and, for production-ready flows, the Wallet Unit Attestation). Created: SCA-User, SCA-IBAN and IBAN Ownership for CZ, GR, IT and RO - issued in SD-JWT (optionally mdoc), device-bound and supporting selective disclosure.
Countries involved	Issuing bank countries: CZ, GR, IT, RO Wallet provider countries: BE, CZ, DE, LU, PL
Number of relying parties	6 banks: National Bank of Greece (GR), Banca Sella (IT), Banca Transilvania (RO), Air Bank, Komerční Banka and ČSOB (CZ), supported by EAA issuers Bank ID CZ and Mastercard.

Table 3: PA1 Scenario 4

Name	Update KYC information
Description	An already onboarded customer updates its customer information through the EUDI Wallet. The MVP is limited to updating the Place of Residence: after session-level SCA at the bank's online channel, the customer presents an updated Place of Residence attestation, issued for the pilot as a QEAA by a QTSP (InfoCert for IT, IDnow for DE and GR) in the absence of authentic sources. The bank verifies the attestation and authorises the specific data change through a dedicated SCA with transaction-specific binding (PSD2 Art. 97, RTS Art. 26, PSR Art. 85) before updating its CRM and core banking systems. Annual Income and Occupation updates are MVP+.

Setting	Remote, via the bank's online channel, with a mock bank application acting as relying party in a single interoperability pilot; same-device (deep link or DC APIs) and cross-device (QR) flows; both customer-initiated and bank-initiated triggers.
Wallet types used	EUDI Wallet for natural persons only
Attestations used	Consumed: PID and the User-level SCA attestation (as finalised in PA1 Scenario 4, with the existing bank SCA method as fallback). Created: Place of Residence attestation (QEAA, SD-JWT VC, default validity 12 months, selective disclosure of street, number, postal code, city and country).
Countries involved	IT, GR, DE.
Number of relying parties	1 - a mock bank application acting as relying party across the three pilot countries and provided by OneSpan; QTSP issuers InfoCert (IT) and IDnow Trust Services (DE/GR).

Table 4: PA1 Scenario 5

In summary, the four PA1 scenarios form a coherent consumer banking journey: cross-border account opening (with and without an intermediary), contract signing with QES, issuance of banking attestations (SCA-User, SCA-IBAN, IBAN Ownership) and digital wallet-based updates of KYC data. The attestations issued in Scenario 4 are a key enabler both for the other PA1 scenarios and for the PA2 payment scenarios. The main challenges are evolving standards (ARF, TS12, OpenID4VP/VCI), the absence of authentic sources for several KYC attestations (mitigated with QTSP-issued synthetic attestations) and open regulatory questions on SCA for data changes, which are being escalated to the financial supervisory authorities.

4.2.2 Use case PA2 – Consumer payments

The purpose of this use case is to demonstrate the use of the EUDI Wallet in consumer payments, both as an alternative Strong Customer Authentication (SCA) method in existing payment flows and as a means of payment initiation. As discussed above financial services are explicitly obliged under **eIDAS 2 Article 5f(2)** to accept the EUDIW for Strong Customer Authentication.

PA2 is structured along two dimensions: **payment authentication (SCA) vs. payment initiation**, and **card vs. account-to-account (A2A)** rails.

- **A.1 – A2A Online SCA (lead: Tink):** EUDIW used as the SCA method for banking payments under PSD2, keeping the existing PISP flow intact.
- **A.2 – A2A Payment Initiation (lead: BankID.cz):** An **IBAN credential stored in the EUDIW** is shared with the merchant at checkout via a new "Pay with EUDIW" acceptance mark to initiate an account-to-account payment.
- **B.1 – Card Online SCA (lead: Visa):** EUDIW used as the SCA method for "Pay by card" transactions, integrated with existing 3-D Secure infrastructure.
- **B.2 – Card Payment Initiation (lead: Mastercard):** A digital **card credential stored in the EUDIW** is shared with the merchant at checkout to initiate a card payment.

It covers the two dominant payment rails: account-to-account (A2A) 'Pay-by-Bank' payments via Open Banking, and card payments. In the SCA scenarios (A1 and B1) the bank remains the relying party and invokes the EUDI wallet to authenticate its own customer during payment authorisation, using a bank-issued SCA attestation (SCA-IBAN, SCA-Card/Digital Payment Credential or SCA-User). In the payment-initiation scenarios (A2 and B2) the merchant or its PISP is the relying party: the EUDI wallet presents a payment-instrument-bound attestation with the transaction data cryptographically bound to it, optionally combined with additional credentials such as a loyalty or student card. All scenarios build on ARF Technical Specification 12 (TS12), use the W3C Digital Credentials API as the preferred EUDI wallet invocation mechanism with deep link / Custom URI as fallback, and rely on SCA attestations issued by banks under PA1 Scenario 4. (There is no dependency on PA1; for relying partners that are not part of PA1, the required SCA attestations will be issued in PA2.)

Our vision is that the EUDIW can be used to check out in an eCommerce transaction. In a single interaction, the EUDI wallet verifies the merchant's authenticity via the Relying Party Trust List, presents a digital payment credential and any additional identity attributes required (e.g. driving licence, age, student status), and authenticates the user biometrically on the mobile device. Leveraging W3C Digital Credential APIs, the flow avoids app-switching, delivering a materially better user experience than today's redirect-based journeys and unlocking adjacent experiences such as convenient and privacy preserving identity or eligibility (e.g. Student status) verification.

Desired outcomes for PA2 and questions to explore:

- **Industry readiness for EUDI wallet-based SCA**, with concrete guidelines aligned to eIDAS 2 Art. 5f, PSD2 and the emerging PSR — without requiring outsourcing agreements between PSPs and digital wallet providers.
- **Proof that the EUDIW can also initiate payments** on both card and A2A rails, including the consideration existing acceptance marks and infrastructure
- **Enrich payments with identity attributes**, enabling new commerce experiences.
- **Alignment with and shared learnings with standards across ARF/TS12, EMVCo, FIDO, SRC, OpenID and Berlin Group.**
- **Evidence and learnings on risk, fraud and liability allocation** between EUDI wallet providers, PSPs and merchants.
- **Insights on adjacent innovations** — agentic commerce, stablecoins and payment wallets.
- **Compatibility with existing infrastructure**, including 3-D Secure, tokens, Click To Pay (SRC), PSD2 APIs and current e-commerce integrations, as a prerequisite for scale.

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	Account to account online SCA (A1)
Description	Issuer-requested ('bank-led') Strong Customer Authentication for Open Banking account-to-account 'Pay-by-Bank' payments: during payment authorisation the bank invokes the consumer's EUDI Wallet, which presents the SCA-IBAN attestation previously issued by that bank. The bank verifies the attestation, completes the SCA step and proceeds with the payment

	under existing Open Banking and SEPA flows; merchants and PISPs have no interaction with the digital wallet and are only informed of the payment outcome. Cross-border interoperability is demonstrated by locating the merchant in a different Member State than the consumer, bank and digital wallet.
Setting	Remote, same-device journey at an online merchant checkout; digital wallet invocation via DC API where supported, deep link as fallback. Cross-device journeys and the SCA-User attestation are MVP+.
Wallet types used	Natural Person EUDI Wallet only; Business Wallets are out of scope.
Attestations used	Consumed: SCA-IBAN (or SCA-User) (attestation specification by WP3 T&S, issuance specification in PA1 Scenario 4, issued and verified by the same participating PA2 bank). No attestations are created within the scenario.
Countries involved	Issuing and relying-party (bank) countries: GR, CZ; merchants and PISPs operate EU-wide.
Number of relying parties	2 banks: National Bank of Greece (GR) and Komerční banka (CZ); merchants Cyclades Fast Ferries and Google; PISPs Mastercard Open Banking Services EU and Tink; wallet provider Aricoma (CZ).

Table 5: PA2 Scenario A1

Name	Account to account payment initiation (A2)
Description	Cross-border account-to-account payment initiation at an online merchant's checkout: the holder selects 'Pay with EU Digital Identity Wallet', the digital wallet presents the SCA-IBAN attestation with the transaction data (amount, payee, reference) cryptographically bound to it per TS12, the merchant or its PISP verifies the presentation and submits a Signed Transaction Request to the bank's new API, and the bank executes the A2A credit transfer (using SEPA). An optional combined presentation of a Loyalty Card or Student Card alongside the SCA-IBAN attestation is included.
Setting	Remote checkout; W3C DC API as the primary same-device invocation with Custom URI/deep link as fallback, plus cross-device (QR) variants; EUR transactions only; Android devices for the pilot.
Wallet types used	Natural Person EUDI Wallet (Aricoma reference wallet, iGrant.io).
Attestations used	Consumed: SCA-IBAN (issued via PA1), optionally SCA-User, optionally Loyalty Card (Fast Ferries) and Student Card (University of the Aegean). No attestations are created within the scenario.
Countries involved	Issuing (bank) country: CZ. Relying party (merchant) country: GR; cross-border combinations GR-CZ.
Number of relying parties	2 merchant relying parties - Cyclades Fast Ferries (GR) and Google - with UAegean as intermediary, PISPs Google and Worldline, and issuing banks Air Bank and Komerční banka (CZ).

Table 6: PA2 Scenario A2

Name	Card online SCA (B1)
Description	Use of the EUDI Wallet to authenticate online card payments ('pay by card') in issuer-requested flows, anticipating the eIDAS2 obligation for EU banks to offer the EUDIW as an alternative SCA method for online payments by end of

	2027. Two MVP flows are piloted: (1) registration, in which the consumer registers the digital wallet with the bank from the bank portal, resulting in issuance of an SCA attestation; and (2) payment SCA, in which the bank (or an intermediary acting on its behalf) invokes the digital wallet within the EMV 3DS or token authentication flow and the EUDI wallet returns the SCA attestation together with signed dynamic-linking evidence. Two attestation types are evaluated: a card-level SCA-Card (Digital Payment Credential, based on EMVCo DPC Draft 1.0) and a user-level SCA-User ('Bank Key').
Setting	Remote; same-device flows via DC API (cross-device QR as variation, Custom URI as fallback); real payment transactions with real cards at real merchants in a controlled pre-production environment.
Wallet types used	Natural Person EUDI Wallets (Google Wallet, GRNET, iGrant.io, Veridas).
Attestations used	Consumed: PID, or a derived PID issued from a passport by a private wallet (RO, NO, ES). Issued: SCA-Card v1.0 (DPC) for RO and NO, and SCA-User v1.0 ('Bank Key') for ES, issued as EAAs by TSPs (no qualified services required for the pilot).
Countries involved	Issuing and relying party (bank and consumer) countries: RO, NO, ES. Merchant) countries: GR plus the Netflix test markets (approx. 3 countries, to be confirmed).
Number of relying parties	3 issuing banks acting as relying parties: Banca Transilvania (RO), Sparebank 1 (NO) and CaixaBank (ES), supported by intermediaries Visa and Veridas; merchants Netflix and Cyclades Fast Ferries (merchants are not relying parties in this scenario)

Table 7: PA2 Scenario B1

Name	Card payment (B2)
Description	Card-based payment initiation ('guest checkout') where the consumer selects 'EU Digital Identity Wallet' as a payment option in the merchant checkout. Three MVP flows: (1) provisioning of the Digital Payment Credential (DPC) into the digital wallet, with the card network acting as EAA provider on behalf of the issuing bank and a new Credential Issuance Facilitator role orchestrating issuance via the card network tokenisation system; (2) guest checkout at an eCommerce merchant, in which the DPC presentation identifies the selected card token and provides cryptographic proof of strong user authentication and transaction intent; and (3) enhanced guest checkout, combining the DPC with a 'proof of eligibility' presentation (e.g. Student ID or Loyalty Card). The card network acts as Validator-TSP, verifying the DPC and returning transaction credentials (token, cryptogram) for payment authorisation.
Setting	Remote, mobile (Android) same-device flows via DC API with Custom URI as fallback (iOS via Custom URI); cross-device considered as a variation; Trust List simulation provided by WP4.
Wallet types used	Natural Person EUDI Wallets (iGrant.io, Walt.id, Google).
Attestations used	Consumed: PID, Student ID attestation (GR) and Loyalty Card attestation (GR) for the combined presentation.

	Issued: Digital Payment Credential (DPC / SCA-Card, SD-JWT VC) for FI.
Countries involved	Issuing (bank) country: FI. Relying party (merchant) countries: FI and GR.
Number of relying parties	2 merchant relying parties: Cyclades Fast Ferries with the University of the Aegean (GR) and Google (FI); issuing bank OP Bank (FI); Mastercard as EAA provider and Validator-TSP; G+D Netcetera as Credential Issuance Facilitator.

Table 8: PA2 Scenario B2

In summary, the four PA2 scenarios cover the consumer payment landscape across both rails (account-based and card-based) and both roles of the EUDI wallet (authentication and payment initiation). They share a common technical foundation - TS12-based SCA attestations issued by banks in PA1, SD-JWT VC format, OpenID4VP with DC API invocation - allowing learnings on attestation reuse, dynamic linking / transaction data binding and checkout UX to be compared across scenarios. The main dependencies are the maturity of TS12, the maturity of the DC API, and the issuance of SCA attestations by banks participating in both PA1 and PA2. The outcomes and findings from the piloting will be shared with the European Commission as recommendations to improve TS12.

4.2.3 Use case PA3 – Business bank account opening

The purpose of this use case is to demonstrate the cross-border onboarding of a registered EU company at a bank in another Member State using the European Business Wallet (EBW) in combination with the EUDI Wallet, in line with the Anti-Money Laundering Regulation (EU) 2024/1624 that applies in full from July 2027. A natural person (the initiator) identifies with the PID in their EUDI Wallet, while the legal entity presents company attestations (EBWOID, EUCC, VAT, tax data and ownership, control and UBO information) from its EBW. The use case continues with the digital signing of the account contract by the legal representatives using a QES from their EUDI Wallet and concludes with the bank issuing an IBAN Ownership Verification (IBAN-OV) attestation into the company's EBW, which can be reused by other use cases (e.g. PA4). The MVP focuses on a one-person company structure (the initiator is simultaneously the legal representative, UBO and contact person), covering typical SME and sole-trader cases; complex ownership and control structures are addressed in MVP+.

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	Cross border account opening
Description	A registered company in Country A opens a business bank account in another EU Member State using the European Business Wallet (EBW) and the EUDI Wallet, in line with the upcoming AMLR (EU) 2024/1624 data requirements. The initiator identifies with the PID from their EUDI Wallet; the bank verifies the EBWOID and EUCC from the company's EBW, checks that the initiator is a legal representative named in the EUCC, automatically requests VAT, Tax ID (sole traders), Company Info and Contact Person, and verifies the Ownership, Control and UBO lists - comparing the company-issued UBO list with a UBO list issued by a QTSP over the transparency

	register - before verifying the UBOs via their PIDs and cross-checking all data. The MVP builds on BU1 (WP2) and covers low/medium-risk, standalone one-person companies (initiator = legal representative = UBO = contact person); sanction and PEP screening are out of MVP scope.
Setting	Remote onboarding via a (mocked) banking landing page; interplay of the EUDI Wallet (natural persons) and the EBW (legal entity); WE BUILD trust infrastructure for attestation validation.
Wallet types used	EUDI Wallet (natural person) and European Business Wallet (legal person).
Attestations used	Provided by authentic sources: EBWOID, EUCC, Tax Number, Tax ID, UBO List (QTSP over the transparency register). Provided as EAs: VAT, Company Info, Contact Person. Issued by the company's EBW: Ownership List, Control List, UBO List and Signatory Rights.
Countries involved	Confirmed relying-party (bank) countries: DE, IT, CZ (PL, NL, RO and AT to be confirmed). Holder (company) countries: AT, CH, CZ, DE, FR, IT, NL, PL.
Number of relying parties	3 confirmed banks - Deutsche Bank (DE), Banca Sella (IT) and Czech banks currently being onboarded (CZ) - with ABN AMRO (NL), a Polish bank (PL), Banca Transilvania (RO) and RBI (AT) to be confirmed; intermediaries/technology providers InfoCert, BankID, Doxallia and PWPW.

Table 9: PA3 Scenario 1

Name	Digital signature
Description	After successful onboarding (PA3 Scenario 1), the legal representative(s) sign the bank account contract. The bank derives the signatories from the EUCC (a separate Signatory Rights attestation is not required), prepares the contract in the bank portal, verifies each legal representative via the PID from their EUDI Wallet and lets them sign with a QES from their EUDI Wallet; the signed contract is then shared back to the company's EBW. Working assumption: a digital wallet-centric model with the bank portal as external Signature Creation Application forwarding to a remote QSCD; the QTSP-centric model is available as fall-back.
Setting	Remote signing from the bank portal acting as Signature Creation Application (CSC API v2.2); interplay of the bank's EBW, the company's EBW and the legal representatives' EUDI Wallets.
Wallet types used	EUDI Wallet (legal representatives) and European Business Wallets (bank and company).
Attestations used	Consumed: EUCC (issued in Scenario 1 by the business registers) and PID; QES issued to the legal representatives by QTSPs upon presentation of the PID. No attestations are issued in this scenario.
Countries involved	DE, NL, PL.
Number of relying parties	3 banks: Deutsche Bank (DE); ABN AMRO (NL) and Pekao SA (PL) to be confirmed. Holder companies: Bosch NL, Bosch DE and Identonic (PL).

Table 10: PA3 Scenario 2

Name	Bank-issued attestations
------	--------------------------

Description	Directly after account opening, the bank issues an IBAN Ownership Verification (IBAN-OV) attestation into the company's EBW, acting as both credential issuer and authentic source. The IBAN-OV attestation provides third parties with trusted assurance that a specific IBAN is legally owned by a designated legal entity; it is not used to initiate or execute payments and can be reused across business processes (e.g. PA4 and onboarding flows) until revoked. MVP: synchronous issuance in the still-active session by the sole legal representative; MVP+: asynchronous issuance triggered weeks later by any authorised person.
Setting	Remote, via the bank's portal in the session established during account opening (Scenarios 1 and 2, so the identification phase is skipped); issuance via OpenID4VCI with an advanced electronic seal (self-issued EAA).
Wallet types used	European Business Wallet (company) in combination with the EUDI Wallet identification of the acting natural person.
Attestations used	Consumed (pre-conditions from Scenarios 1-2 and BU1): PID, EBWID, EUCC, Tax Number/Tax ID, LEI, UBO/Control/Ownership Lists, Company Info, Contact Person, Signatory Rights. Created: IBAN-OV attestation (EAA).
Countries involved	Issuing country: DE. Holder country: NL.
Number of relying parties	1 issuing bank: Deutsche Bank AG (DE); holder Robert Bosch B.V. (NL); wallet providers Procivis (EUDI Wallet) and Spherity (EBW).

Table 11: PA3 Scenario 3

In summary, the three PA3 scenarios form one sequential end-to-end journey - business account opening, contract signing and IBAN-OV issuance - executed in the MVP by a single natural person acting for a one-person company. The journey exercises the interplay between EUDI Wallets and Business Wallets, AMLR-aligned KYB data, QES and bank-issued attestations, with the IBAN-OV output feeding directly into PA4. The main dependencies are the BU1 flow in Work Package 2 (issuance of the company attestations), the availability of authentic sources per country and the maturity of the WE BUILD trust infrastructure; verification steps not implemented in the MVP shift the associated liability to the relying party until they are completed in MVP+.

Desired outcomes for PA3 and questions to explore:

- Demonstrate the use of EUDIW and EUBW for cross-border opening of a business bank account in **compliance with AMLR requirements** for customer identification
- **Assess availability of required attestations from authentic sources** – and whether this is likely to become a key challenge to adoption and scaling in the markets piloted

Evaluate and pilot **interactions between EUDIW and EUBW** for the purpose of demonstrating mandate and signing in terms of challenges, user experience, security requirements, and business process implications

4.2.4 Use case PA4 – Business payments

The purpose of this use case is to demonstrate how the EUDI Wallet and the European Business Wallet can transform business-to-business (B2B) payment processes by issuing a standardised, verifiable eReceipt attestation that reliably links each payment transaction to a structured proof

usable by banks, merchants and third parties (accounting, tax, expense management). Two payment workflows are covered: Scenario 1.1 - an online purchase paid by corporate card where the invoice is deferred, from Strong Customer Authentication (reusing PA2) through settlement to eReceipt issuance; and Scenario 1.2 - an IBAN payment (SEPA credit transfer) of an upfront eInvoice, linking the invoice, the payment order and the eReceipt. Both scenarios follow the same six-step flow (legal-entity selection, payment initiation, personal authorisation, legal-entity authorisation via Signatory Rights / Power of Attorney, settlement, eReceipt issuance), with the eReceipt delivered as a company-level artefact into the buyer's EBW.

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	eInvoicing payment and eReceipt issuance – card payment
Description	B2B payments with verifiable proof of payment. This scenario handles card payment of a deferred invoice: the authorised person pays a retail-style online purchase by a corporate card with EUDI Wallet SCA (as defined in PA2), and after settlement, a standardised eReceipt attestation is issued into the buyer company's EBW. Flow: legal-entity selection, payment initiation, personal authorisation (SCA), legal-entity authorisation (SR/PoA), settlement and eReceipt issuance. The eReceipt (DS-011) is a company-level artefact stored in the Business Wallet and is complemented by a bank-issued Payment Attestation (DS-012), an eReceipt Routing Credential (DS-013) and an Invoice Payment Confirmation (IPC).
Setting	Remote B2B purchases (e.g. ferry tickets via a booking platform); the authorised person is authenticated for the card payment; eReceipt issuance via OpenID4VCI, aligned with CEN/TS 16931-8:2024 and EN 16931.
Wallet types used	EUDI Wallet for the authorised person to perform SCA; European Business Wallets for the buyer and seller companies.
Attestations used	Consumed: PID, EBWID, EUCC, IBAN Attestation (from PA3 Scenarios 1/3), SCA Attestation (PA2 B1 / PA3 / issuing bank), KYS supplier onboarding (BU1, Scenario 1.1 only) and the eInvoice (Peppol BIS Billing 3.0 / EN 16931). Issued: DS-011 eReceipt, DS-012 Payment Attestation, DS-013 eReceipt Routing Credential and IPC (Invoice Payment Confirmation).
Countries involved	Scenario 1.1: seller GR (Cyclades Fast Ferries); buyers FI (sole trader) and GR (travel agent); card attestation FI (OP Bank); eReceipt intermediary FI (ReceiptHero).
Number of relying parties	3 buyer relying parties for the eReceipt: a Finnish sole trader and a Greek travel agent (both via the Bootes booking platform), supported by intermediaries UAegean, Worldline, ReceiptHero and DATEV.

Table 12: PA4 Scenario 1.1

Name	eInvoicing payment and eReceipt issuance – account payment
Description	B2B payments with verifiable proof of payment from a bank account (IBAN payment, upfront invoice): the eInvoice is received in the buyer's EBW, the SEPA credit transfer is initiated and authorised (token-based for standard

	payments, Signatory Rights and Power of Attorney checks for high-value payments), and the eReceipt links the Peppol invoice to the SEPA payment. Both follow the same six-step flow: legal-entity selection, payment initiation, personal authorisation (SCA), legal-entity authorisation (SR/PoA), settlement and eReceipt issuance. The eReceipt (DS-011) is a company-level artefact stored in the Business Wallet and is complemented by a bank-issued Payment Attestation (DS-012), an eReceipt Routing Credential (DS-013) and an Invoice Payment Confirmation (IPC).
Setting	Remote B2B purchases (e.g. ferry tickets via a booking platform; ERP-generated credit transfers); the authorised person is authenticated to the bank channel; eReceipt issuance via OpenID4VCI, aligned with CEN/TS 16931-8:2024 and EN 16931.
Wallet types used	EUDI Wallet for the authorised person; European Business Wallets for the buyer and seller companies.
Attestations used	Consumed: PID, EBWID, EUCC, IBAN Attestation (from PA3 Scenarios 1/3), SCA Attestation (PA2 B1 / PA3 / issuing bank), KYS supplier onboarding and the eInvoice (Peppol BIS Billing 3.0 / EN 16931). Issued: DS-011 eReceipt, DS-012 Payment Attestation, DS-013 eReceipt Routing Credential and IPC (Invoice Payment Confirmation).
Countries involved	Seller DE (Bosch); buyer DE or CH (SME to be identified); IBAN attestation DE (Deutsche Bank). Wallet providers in SE and CH.
Number of relying parties	3 buyer relying parties for the eReceipt: German/Swiss SME, supported by intermediaries UAegean, Worldline, ReceiptHero and DATEV.

Table 13: PA4 Scenario 1.2

In summary, PA4 demonstrates that the eReceipt model works on both card and account-to-account rails and that a structured, verifiable receipt can be issued into, stored in and reused from a Business Wallet. The scenarios depend on upstream results from PA3 (IBAN attestation), PA2 (card SCA) and BU1 (Know-Your-Supplier onboarding), and on the evolving eInvoicing standards landscape (EN 16931-1:2026 and CEN/TS 16931-8:2024) analysed in the scenario specifications.

Learning objectives

- Demonstrate how EUDIW and EUBW (EU Business wallet) bring value to business payments services such as eInvoicing, eReceipts and government tax disbursements as they relate to supply chain and expense management.
- Evaluate the benefits and challenges in verifying Seller and Buyer using a EUBW and EUDIW
- Evaluate how interactions between EUDIW and EUBW can be performed considering user experience, security and impact on business processes for different payment flows (e.g. account and card payments)

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 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.

- Exceptions and variations

In general, all use cases were directed to focus on the core of the process and to pay less attention to exceptions and technical errors. This reflects WE BUILDs aim of learning about the value of processes across industries, creating best practices, and providing feedback to the ARF and the Implementing Acts, rather than delivering exhaustively hardened production flows.

- Key-objectives

In line with the Grant Agreement, the use cases focused on learning about the value, feasibility and process complexity of using the (business) wallet across different industries and situations. The six WE BUILD key objectives guided the detailing of the scenarios, namely to: (1) test out the wallet ecosystem in real processes; (2) provide recommendations to the ARF, Implementing Acts and standards bodies; (3) build a foundation for the European Business Wallet; (4) re-use results from previous Large-Scale Pilots; (5) increase infrastructure maturity towards large-scale adoption; and (6) connect with other European infrastructures. The intent is to fulfil these objectives within the pilot scope. Other topics, such as data protection, were of secondary concern (without diminishing their importance) and were addressed once the primary objectives had been secured.

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.

- Attestation formats

The use cases start from SD-JWT VC and, where needed, mdoc; in WP3 only SD-JWT VC is used. Both formats are consistent with ARF TS12, which supports SD-JWT-VC key binding and mdoc (ISO/IEC 18013-5) device authentication for the SCA signature. For every attestation, a rulebook defines the meaning of all attributes and structures to ensure interoperability across the ecosystem. Rulebooks are produced at version 1.0 to allow implementation to start; version 2.0 is expected early in the implementation phase, bringing semantic improvements without changing the structure or nature of the attestations. Time permitting, other formats (e.g. JSON-LD) may be explored later, although this is unlikely for the WP3 use cases.

- Pilot ambition

In LSPs there is an inherent tension between solutions that are fully ready for real-world use – covering all complexity and every exception – and solutions that are feasible and good

enough to pilot. Feasibility is largely determined by the available time, resources, and the number and expertise of partners. The use cases therefore balanced real-world requirements against pilot feasibility: on one hand seeking interoperability with existing infrastructure, systems and standards that are essential for scaling; on the other experimenting with the innovation opportunities enabled by wallets, verifiable credentials and the new trust framework. As a result, much will be learned for a future full-scale roll-out, while in some areas additional enhancements will still be needed to make the solutions “real-world-proof”.

5.2 Main working assumptions

Many working assumptions were made in the use cases. Some very specific for the 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.

- Banks stay in charge of risk and compliance

whether a payment or contract is acceptable and for meeting their regulatory obligations (PSD2/PSR, card scheme rules, AMLR), even when the EUDI Wallet is used for strong authentication. These are the key principles that keep wallet-based SCA from being treated as delegated and therefore avoid any outsourcing requirement, in line with the Commission Q&A and Chapter 4. In concrete terms:

- In **account-to-account payments**, the bank invokes the wallet as the SCA method and verifies the resulting authentication code, but continues to run its own fraud and risk engine and retains legal responsibility; that responsibility does not move to the wallet provider. This corresponds to the TS12 two-party, issuer-requested model.
- In **card payments**, the issuing bank (or an intermediary/Validator-TSP acting on its behalf) verifies the wallet-generated authentication code – i.e. the transaction data signed under device binding – within the existing EMV 3DS / tokenisation flow and then approves or declines. The pilot tests the eIDAS 2 Article 5f(2) obligation for banks to accept the EUDIW

as an SCA method on the user's request; it does not assume any authentication liability is transferred to the wallet.

- In **corporate banking**, the bank remains the party that relies on digital signatures and company data to open accounts and sign contracts. The wallet helps establish who signs and on whose behalf, but the onboarding decision remains the bank's.

Whether, and which, wallet-generated **risk and assurance signals** a bank can consume to support its risk decision (as anticipated by PSR Art. 83 on transaction monitoring and by Chapter 4) remains an open research topic: standardised signals are not yet available from the wallet ecosystems being deployed, so for the pilots the bank relies on its existing controls. This assumption keeps the trust model close to how banking works today, which makes the pilots easier to position with banks and regulators.

- One common way of “user approval” that can be reused
Whenever a user approves something important – a payment, a card transaction, or a contract – the approval is captured using the single TS12 dynamic-linking mechanism. The relying party sends a presentation request that includes the transaction data (for payments, at least the amount and the payee). The wallet renders that data to the user in a read-only, secure view (the “what you see is what you sign” principle), the user approves with at least two independent authentication factors, and the wallet includes a representation of the transaction data in the signature created for device binding. The resulting signature is the authentication code that satisfies the PSD2 dynamic-linking requirement. Because the same mechanism is reused everywhere, solutions built for one use case extend directly to others:
 - In **A2A payments**, the signed transaction data proves that a specific payment (amount and payee, bound to the account attestation) was approved by the account holder in their wallet – the basis on which the bank executes the transfer.
 - In **card payments**, the same mechanism provides dynamic linking: the issuer (or its Validator-TSP) can verify exactly which card transaction the user confirmed in the wallet, not merely that the user authenticated.
 - In **corporate scenarios**, the same pattern shows that a named legal representative, acting for a specific company, approved a particular version of a contract (the document hash is rendered and bound under WYSIWYS before the QES is created).
- The pilot aims for simple subset of the TS12 datamodel first

The pilots deliberately concentrate on the simplest, most common cases: euro payments, one-off transactions with a fixed amount, and a limited number of partners and countries. This is a scoping choice within the richer TS12 model rather than a limitation of it – TS12 also supports recurring payments and e-mandates (urn:eudi:sca:emandate:1: single, deferred and recurring), estimated and earmarked amounts, merchant-initiated transactions and instalments, which are deferred to later phases. Concretely:

- In consumer **A2A payments**, flows are written for straightforward euro account-to-account payments, with no foreign exchange, no instalments and no change of amount after the wallet step.

- In **card payments**, the focus is on ordinary online purchases rather than subscriptions, split payments or discount logic that would change the amount after the user has approved it.
- In **corporate banking**, the pilot concentrates on a simple company structure (e.g. a single legal representative signing) and a limited set of cross-border combinations, rather than all corporate structures from day one.

This lets the project prove the core ideas in practice without being blocked by edge cases, while remaining forward-compatible with the full TS12 data model.

- 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, but in the context of piloting a necessary prerequisite for execution of the process.

- Mandate related attestations

Several use cases rely on mandate-related attestations. WE BUILD uses three types to validate a mandate (even though other attestations may partially carry such information). Note that these attestations concern authorisation/representation and are outside the scope of TS12, which governs payment SCA; they are used in the PA3/PA4 authorisation steps.

- 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 (EBWID), 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 3 applies a domain perspective within these objectives, looking for lessons and recommendations to increase adoption and scalability within the PAYMENTS 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 sector systems*

Learn how digital wallet-based identification, authentication and authorisation can be integrated with existing retail banking onboarding processes without major disruption.

Learn how digital wallet-based trust can be integrated into Open Banking A2A SCA, and SCA using 3DS and tokens, and payment-initiation stacks, including how EUDIW-based SCA or signed transaction requests coexist with existing PSD2 authentication, consent and risk-management components.

Learn what it really takes to keep SCA and banking attestations trustworthy over time (revocation of SCA-IBAN, account closure, change of bank relationship, digital wallet compromise) in dynamic, cross-border consumer contexts, reusing BU/SC lifecycle and revocation learning goals.

6.2 *Attestation usage across processes*

Understand how a shared set of attestations (identity, representation, tax, business attributes, etc.) can be reused across multiple banking processes and contexts—such as onboarding, ongoing due diligence, cross-border account opening—and what constraints or extensions are needed to make this reuse practical.

Learn how SCA-User and SCA-IBAN attestations can be reused across different payment flows and channels (issuer-requested SCA vs merchant/PISP-captured flows) while keeping issuance and lifecycle manageable for banks, holders and relying parties.

6.3 *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. Learn how same-device and cross-device flows using different technologies like DC API and Custom URI/deep-link affect sequencing, error handling and fall-back behaviour. The goal is to identify robust patterns for sequencing, error handling and fall-back options while keeping the overall interaction as simple as possible for end users.

6.4 User Experience

Assess how consumers perceive digital wallet-based bank account opening compared to traditional digital onboarding (document uploads, in-app KYC), focusing on clarity of consent, perceived safety, and overall effort.

Assess how consumers perceive digital wallet-based SCA and payment initiation compared to bank-app authentication and existing payment flows (3DS, bank redirect), including error recovery, device switching and combined-presentation UX (e.g. payment + loyalty).

6.5 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.

Understand how emerging standards such as TS12, SD-JWT VC profiles for SCA, and IBAN Ownership schemas behave in practice, and where pilots should feed specific recommendations back into ARF and payments standardisation.

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 3. 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 3.

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.

Next to that, more payment-specific frameworks and regulations apply to the use cases in this work package. During the specification phase, TS12 was identified as one of the specifications that is under development but is of great importance for the implementation of the use cases.

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 TS12, 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, close collaboration with standardization bodies is performed as much as possible. The pilots are already working standards bodies that are already undertaking standardisation of relevant attestations (notably EMVCo + FIDO Alliance for the Digital Payment Credential or SCA-Card Attestation as it is called in WE BUILD). Worst case, future versions of regulations and frameworks chose conflicting directions, or gaps / ambiguities remain.

For best control in WE BUILD, the use case maintains 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 to revisit 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 PA3 counts on BU1 (work package 2) to issue a KYC attestations for Germany, so PA3 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.

- Maturity of technology

To establish a smooth user experience, new technologies are being considered like DC API. This technology offers better handling of working with different parts of the ecosystem without confusing the user but is still in its experimental stage. A good user experience is however considered a necessity for adoption of the digital wallet by the masses.

For development new technologies like these can offer big challenges, introduce also (temporary) big limitations and with that form a risk for the success of piloting.

As the main objective for the pilots are learning, experimental technologies will be evaluated when the use of such technologies bring important learnings that outweigh the risks to executing the pilots successfully.

8. Conclusion

This deliverable has established the pilot design for Work Package 3 of WE BUILD, covering digital wallet-enabled use cases in the Payment domain. 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 13 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 opening a bank account for businesses or consumers, to doing payments, 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 the payment domain, but also the business and supply chain domain in work package 2 in WE BUILD. 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, 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 3 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 Payments pilots in WE BUILD. It defines the intended scope, priorities and learning focus for Work Package 3 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 3 deliverable.

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

	PA1	PA2	PA3	PA4
Certificate of Residence				
CompanyInfo				
ContactPerson				
ControlList				
EBWID				
Electronic invoice				
EU PoA				
EUCC				
IBAN Ownership				
Legal Entity Identifier				
Loyalty card				
OwnershipList				
PID				
QES (not country bound)				
SCA Card (Digital Payment Credential)				
SCA-IBAN				
SCA-User				
Signatory Rights				
Student				
Tax ID				
Tax Nr				
Targeted Financial Sanctions				
UBO List				
VAT ID				

Annex B – Use case / country matrix

PA1		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	RP	Issuer	RP	Issuer	RP	Issuer	Issuer	RP	Issuer
	CZ										
	DE										
	ES										
	GR										
	IT										
	NL										
	PL										
	RO										
	SE										

PA2		Scenario A1		Scenario A2		Scenario B1		Scenario B2		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	CZ										
	ES										
	FI										
	GR										
	NO										
	RO										
	US										

PA3		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	AT										
	CH										
	CZ										
	DE										
	IT										
	NL										
	PL										

PA4		Scenario 1.1		Scenario 1.2		Scenario 3		Scenario 4		Scenario 5	
	Country	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer	RP	Issuer
	CH										
	DE										
	FI										
	GR										

Annex C – MVP scenario specification documents

Use Case	Scenario ID	Name
	1	Cross-border bank account opening using intermediary platform
	3	Sign contract
	4	Attestation issuance (SCA, IBAN)
	5	Update KYC information
PA2	A1	A2A online SCA
	A2	A2A payment initiation
	B1	Card online SCA
	B2	Card payment
PA3	1	Cross-border Account Opening
	2	Digital Signature
	3	Bank-issued Attestations
PA4	1.1	eInvoicing payment and eReceipt issuance – card payment
	1.2	eInvoicing payment and eReceipt issuance – account payment

WE BUILD consortium

Specification Scenario 1 – Open a Personal Bank Account

WP3– [PA1] Consumer Banking

Date : 22-06-2026
Version : 1.0
Status : For Review

Index

1	Introduction	3
1.1	<i>Objectives of this document.....</i>	3
1.2	<i>Scenario introduction.....</i>	3
2	Scenario Specification	3
2.1	<i>Introduction</i>	3
2.2	<i>Scenario pre-conditions</i>	4
2.3	<i>Scenario main flow</i>	4
2.3.1	<i>Direct Integration.....</i>	4
2.3.2	<i>Intermediary Integration.....</i>	5
2.4	<i>Scenario additional flows.....</i>	5
2.5	<i>Challenges and barriers</i>	7
2.6	<i>Working Assumptions</i>	8
3	Detailed scenario flow.....	9
3.1	<i>Direct Integration.....</i>	9
3.2	<i>Intermediary Integration</i>	12
4	Roles and participants.....	14
4.1	<i>Scenario roles and participants.....</i>	14
4.2	<i>Additional roles and partners</i>	15
4.3	<i>Target country combinations.....</i>	15
4.4	<i>Requirements.....</i>	15
5	Attestations	16
5.1	<i>Introduction</i>	16
5.2	<i>Attestations to be provided by other UCs/WGs/scenarios.....</i>	16
5.3	<i>Created attestations in the scenario</i>	16
	Annex 1 – Requirements for scenario roles.....	18

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 1, as part of use case 1 in work package 3 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

This scenario describes the bank account opening process in which the EUDI Wallet is used to securely provide identity and KYC-related data to the financial institution.

The scenario is based on the following documentation:

- ARF version: <https://eudi.dev/2.9.0/architecture-and-reference-framework-main/>
- Anti-Money Laundering Regulation (EU) 2024/1624
- Revised Payment Services Directive (EU) 2015/2366 (PSD2)
- Draft Third Payment Services Directive (PSD3) and draft Payment Services Regulation (PSR)
- WE BUILD WP4 Conformance Specifications (WBCS) and
- WE BUILD Architecture Decision Record (ADR's)
- The PA1 stock taking document final version (1.0)
- W3C Verifiable Credentials Data Model
- SD-JWT VC (IETF draft)
- OID4VCI 1.0
- OID4VP 1.0
- EMVco Digital Payment Credential Draft 1.0 (19th Jan 2026)
- ARF v2.8.0 Technical Specification 12
- eIDA2 Regulation on SCA (Recital 62 and Article 5f2)

2 Scenario Specification

2.1 Introduction

This scenario covers the onboarding of a natural person wishing to open a personal bank account (e.g. credit account). The scenario, which is part of the MVP, addresses both cross-border (a resident of Country A opening an account in Country B) and in-country (using the EUDI Wallet for domestic banking) use cases. It targets low-medium risk clients and focuses on fulfilling KYC (Know Your Customer) and Due Diligence requirements as defined in Regulation (EU) 2024/1624.

In this scenario, the relying parties (banking institutions) can either do a direct integration with EUDI Wallets, or utilize an intermediary platform to facilitate the ingestion of wallet data to minimize integration effort.

An MVP+ extension of the basic scenario will also be considered and tested, in which case additional attestations will be asked.

2.2 Scenario pre-conditions

Scenario pre-requisites are:

- One or more valid wallet(s) are made available and loaded with the appropriate PIDs.
- For PIDs, “portrait” and “personal_administrative_number” attributes need to be populated. The “personal_administrative_number” will be treated as the “national identification number” described in article 22 of Regulation (EU) 2024/1624.
- WP4 to timely provide test Wallet instances, PID, trust infrastructure etc.
- Standardization of attestation schemas needed for MVP, mainly PID, Tax ID, Certificate of residence.
- Alignment on the intermediary role and availability of trust infrastructure to test real-world scenarios in compliance with the ARF
- Availability of the intermediary APIs and authorized access to Relying Parties

2.3 Scenario main flow

2.3.1 Direct Integration

In a direct integration model, the Relying Party (RP) connects to EUDI Wallets directly, handling the end-to-end presentation flow, including request construction via OID4VP, wallet authentication, credential verification and trust validation on its own infrastructure.

Prior to initiating the flow, the Relying Party (RP) must obtain the Wallet Relying Party Access Certificate (WRPAC) from an Access CA (provided by WP4) to authenticate itself to EUDI Wallets, and successfully register their use case, including the RP's identity, intended use, and required attributes, in the Registry that will be provided by WP4.

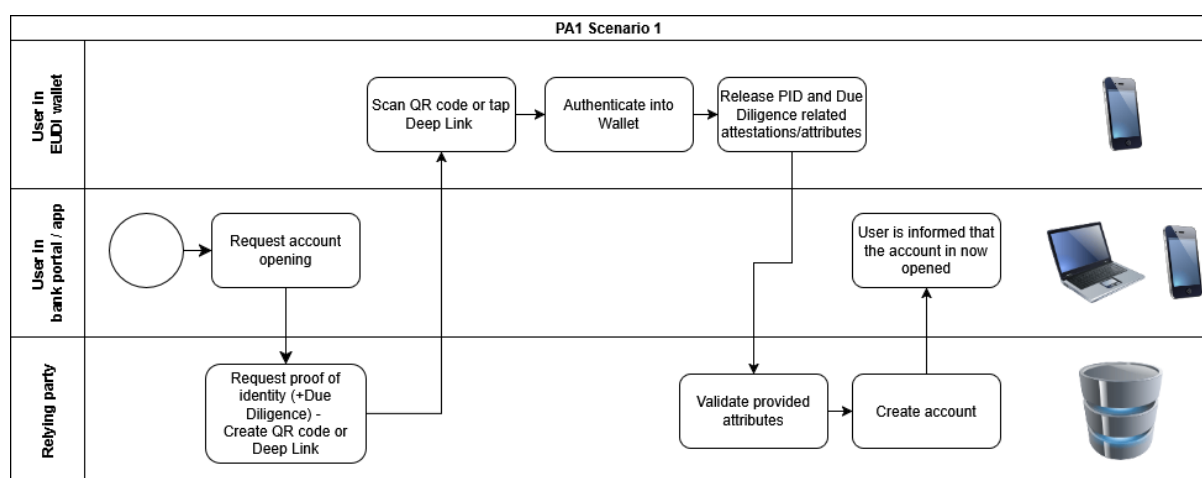


Figure 1 Basic flow for Direct integration

2.3.2 Intermediary Integration

Alternatively, the RP can rely on an Intermediary that manages all wallet interactions on its behalf, where the Intermediary holds its own WRPAC and presents the Wallet Relying Party Registration Certificate (WRPRC) to the wallet, when available, abstracting protocol, trust, verification and operational complexity from the RP.

Prior to initiating the flow, the Intermediary must obtain their WRPAC from an Access CA to authenticate itself to EUDI Wallets, and successfully register the underlying intermediated RP, including the RP's identity, intended use, and required attributes, in the RP Registry that will be provided by WP4.

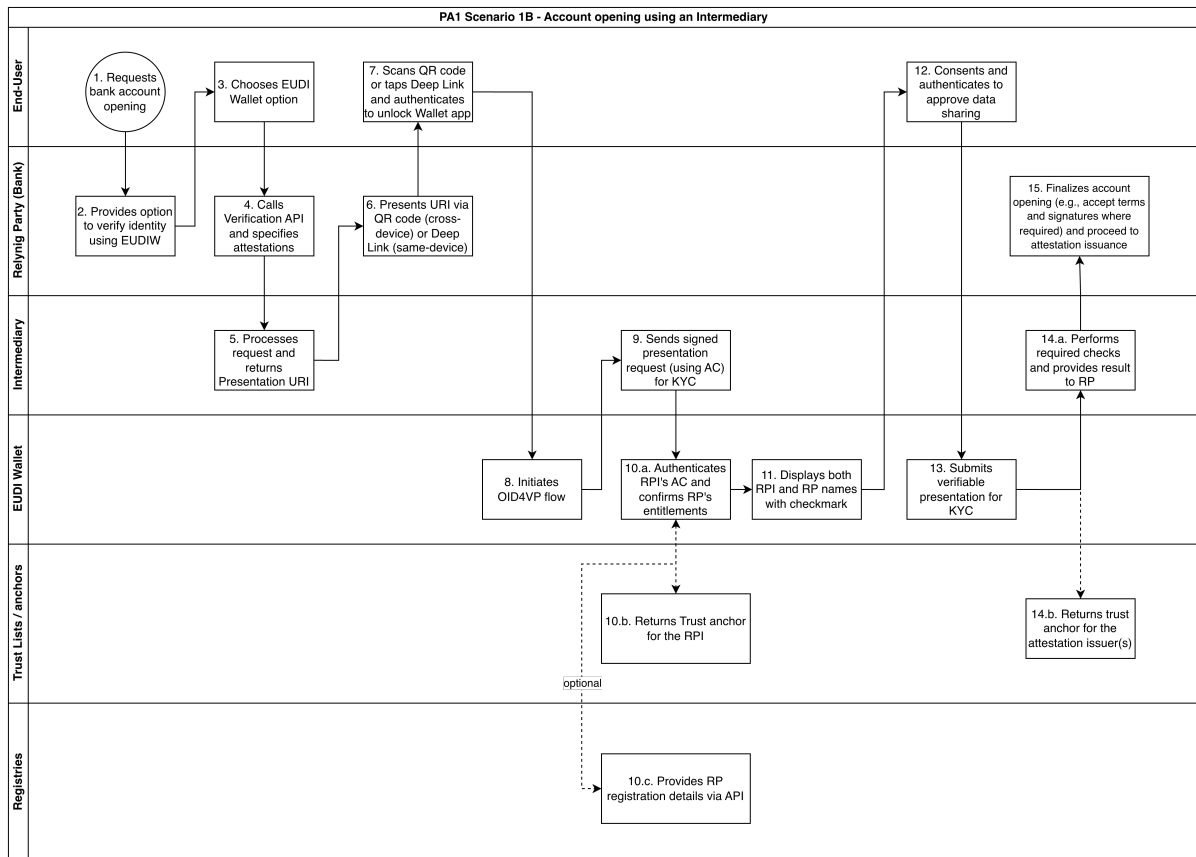


Figure 2 Basic flow for Intermediary integration

2.4 Scenario additional flows

The flows this scenario aims to pilot are depicted in the tables below.

Flow	In /out scope (I/O/E)*	Short description
Basic flows		

- Basic flow – same-device	I	Basic flow to be piloted where Wallet and Relying Party website are present and used on the same device, e.g. smartphone. The DC API (optional) can be used as the standard browser/OS invocation to trigger the wallet presentation, if supported by the Wallet Provider and the browser, and requested by the Relying Party.
- Basic flow – cross-device	I	Basic flow to be piloted where Wallet and Relying Party website are present and used on different devices; for instance: EUDI Wallet on smartphone and Relying Party website on computer or tablet. The DC API (optional) can be used for cross-device presentation, mediated by the browser, if supported by the Wallet Provider and the browser, and requested by the Relying Party.
Alternative flows / Exceptions		
- AF1 – User does not consent to releasing PID and (Q)EAs	I	The user does not consent to releasing the NP PID and attributes from other (Q)EAs. Possible reasons: user doesn't want to share the data or user concludes that the data is not correct and the wallet sends an error message to the relying party. The flow in figure 1 then ends after the step 'Validate proof of identity and due diligence attestations' and the RP informs the User on the outcome.
- AF2 - User exits / cancels flow	I	• The user closes the wallet app before confirming consent • No presentation is produced • RP / Intermediary receives a cancellation/timeout result
- AF3 – PID and/or (Q)EAs revoked	O	The PID of the user or another requested (Q)EAA is revoked, the Relying party doesn't proceed with the process of amount opening. The flow in figure 1 then ends after the step 'Validate proof of identity and due diligence attestations' and the RP informs the User on the outcome.
- AF4 – Required attestation(s) not present in the Wallet	I	• The Wallet does not contain one or more mandatory attestations • Wallet cannot satisfy the presentation request • Flow ends with clear status for missing required attestation(s) • RP decides next step (e.g. fallback option)
- AF5 – Unable to provide certain attributes (due to unavailability or non-applicability) alternative flow	O	The user is unable to provide Tax identification number and/or National identification number mainly due to non-applicability reasons. The RP / intermediary validates the received attributes, and RP requests justification (e.g. via bank's website) on why Tax identification number and/or National identification number were not provided.
- AF6 – Unable to provide mandatory attributes (other than Tax identification number or National identification number)	O	The user is unable to provide mandatory attributes other than Tax identification number or National identification number. The relying party validates the received attributes, identifies the missing ones. The flow in figure 1 then ends after the step 'Validate proof of identity and due diligence attestations' and the RP informs the User on the outcome.
- AF7 - Trust check failure	I	• RP / Intermediary Access Certificate is not authenticated

		• Wallet stops the flow and does not proceed to user consent • Wallet informs the user that the requesting service (i.e. intermediary or RP) is not trusted / verified
- AF8 - Relying Party not registered in the Trust Infrastructure	O	• RP / Intermediary Access Certificate is authenticated • RP has no registration certificate for this use case and is requesting attributes outside of their scope • Wallet detects via the Registrar that RP is exceeding their scope and flags it to the user • Wallet shall allow authorised attributes to be presented to the user for consent; however requests outside registered scope are flagged to the user and should not be disclosed

*I: in scope (MVP), P: parked, O: out of scope, E: scope extension (MVP+)

Other flows or exceptions are not in scope of the pilot and are assumed to be tested and working properly according to specifications, such as:

- Issues regarding non-conformance of [ARF] or other standards, for instance a functional or technical invalid authentication request.
- Issues in the technical connection between the Relying Party and the EUDI Wallet, leading to for instance time-outs.

2.5 Challenges and barriers

The piloting of the natural person onboarding scenario using the EUDI Wallet faces several key challenges related to technical maturity, regulatory uncertainty, and ecosystem readiness, particularly in cross-border contexts and within the MVP scope.

A major challenge is the ongoing evolution of EUDI Wallet-related technical standards (e.g. ARF profiles, OpenID4VP/OpenID4VCI, ETSI/CEN norms). Components reused from previous pilots are often based on older draft versions, while the EUDIW reference implementation continues to evolve. This creates risks of interoperability issues, rework, and delayed integration. In addition, trust management mechanisms (trust lists, revocation, issuer/verifier validation), as well Member state registries to issue Access and/or Registration for Intermediaries and RPs are not yet consistently implemented, limiting reliable cross-border validation. This gap may be mitigated by the trust infrastructure that WP4 is building, including trust lists and registries.

Further challenges arise from missing EU-wide standards and rulebooks for key KYC and Due Diligence attestations, including proof of income or proof of occupation. In some Member States, authentic sources may not be available or digitally accessible. These gaps may require interim solutions such as project-defined credential schemas, simulated authentic sources, or micro-credentials issued as EAs.

Cross-border onboarding is further complicated by national differences in AML, KYC, and banking regulations, increasing implementation effort and potentially limiting the scope of cross-border testing within the MVP.

Finally, the pilot depends on sustained engagement from multiple stakeholders and alignment with the mandated availability of the EUDI Wallet. Combined with evolving requirements, this

creates a risk of delays and unmet KPIs, requiring early prioritization, clear ownership, and fallback options to ensure minimum success criteria.

2.6 Working Assumptions

No specific working assumptions were made.

3 Detailed scenario flow

3.1 Direct Integration

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

Basic flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Other basic flows / alternative flows/ exceptions
Request to open a Personal Bank Account	U	User uses smartphone to open bank app or navigate to bank website. User selects to open a bank account. User chooses to authenticate with the EUDI Wallet. Reference: RP specific.		
Request proof of identity + Due Diligence attestations (TaxID, Certificate of Residence, IBAN Ownership)	RP	The RP creates an Authorization request and provides the user with a deeplink to retrieve the specific Authorization request (same device) or a QR code (cross device). Reference: - WBCS and ADR's - WB Trust framework - UX/UI guidelines		
Authenticate to EUDI Wallet	U	1. The EUDI Wallet is launched on the device and the User gets access to the EUDI Wallet (using identification method as PIN-code for instance). Reference: - EUDI Wallet Provider specific - WBCS and ADR's - UX/UI guidelines		
	U	2. The EUDI Wallet receives the Authorization Request, verifies the		AF7 RP's / Intermediary's Access Certificate fails validation checks.

		signature / RP certificate (Access Certificate) of the request and informs the User on the outcome. Reference: - WBCS and ADR's - WB Trust framework - UX/UI guidelines		Wallet terminates the process and informs User accordingly.
	U	3. The User inspects the Authorization Request. Reference: - WBCS and ADR's - UX/UI guidelines		
Release NP PID and (Q)EAA data	U	1. The User consents to the release of PID and selected (Q)EAA data. Reference: - WBCS and ADR's - UX/UI guidelines		AF1 User does not consent and the wallet sends an access denied error code to the relying party. The process terminates.
		2. The EUDI Wallet sends the Authorization Response with PID and requested (Q)EAAs to the Relying Party.		
		3. The EUDI Wallet returns the User to the Relying Party website or app. Reference: - UX/UI guidelines		Basic flow – cross-device: User is informed to continue on computer or other device.
Validate proof of identity and due diligence attestations (KYC)	RP	The Relying Party checks the validity of the received PID/(Q)EAA attestations.		AF2 Check revocation: PID and /or another (Q)EAA is revoked, bank

		In this basic flow none of the trust checks fails and the process continues. Reference: - WBCS and ADR's - WB Trust framework		terminates the process and informs User accordingly. AF4 Unable to provide certain attributes: The user is unable to provide Tax identification number and/or National identification number mainly due to non-applicability reasons. The user will have to provide justification in RP's Portal. AF5 Unable to provide mandatory attributes: The user is unable to provide mandatory attributes other than Tax identification number or National identification number. The process terminates.
Present terms and conditions	RP	The Relying Party informs the user that the identification and KYC processes have been successfully completed, presents the terms and conditions, and asks the user to confirm their willingness to proceed with the account opening. Reference: - UX/UI guidelines - RP specific		
Accept terms and conditions	U	The User accepts "terms and conditions" and the bank account opening process concludes. Reference: - UX/UI guidelines - RP specific		

3.2 Intermediary Integration

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

Step	Actor	Action	Dependencies	Variations & Exceptions
1	User	Accesses Bank app (web or mobile) and initiates account opening using their EUDI wallet	Bank App/Portal and EUDI Wallet availability	User chooses manual entry
2	Relying Party (Bank)	Triggers KYC request via Intermediary API and specifies required attestation templates and attributes (e.g. PID, Tax ID)	Intermediary API availability RP registration	RP not registered Intermediary unavailable
3	Intermediary	Generates signed Request & provides Link/QR to Bank	Valid AC	AC not available
4	User	Scans QR code or taps deep link to launch Wallet app	Support for cross-device and same-device flows and/or DC API	Device handover
5	Wallet	Verifies intermediary and RP via Registrar API, then displays consent screen showing intermediary & bank name with requested attributes	Registrar API	Trust check failure
6	User	Authenticates (Biometrics/PIN) and consents to data sharing	Attestations (PID, Address, Tax ID)	Consent not given Missing required attestations
7	Wallet	Generates Verifiable Presentation and submits to intermediary	-	Transmission error
8	Intermediary	Verifies presented attestations (e.g. signature, issuer, revocation status, holder	Trust List, Status List	Verification failure

		binding), normalizes data, and forwards it to the bank once verified		
9	Relying Party (Bank)	Receives verified data, completes internal checks, creates user account and proceeds to contract signing to finalize it	-	Internal check failure (Technical)

4 Roles and participants

4.1 Scenario roles and participants

1. Users

MS code	Type of user in scope	User type description
All	Natural person	A European citizen who uses the EUDI Wallet for remote authentication and KYC purposes. This individual seeks to open a bank account cross-border and in-country. A transaction is considered cross-border if the bank is in a country different than the country that issued the Person Identification Data (PID).

2. Relying parties

Overview of relying parties:

MS*	Relying party	Service name	App/ website/ both
CZ	AIR BANK		
CZ	ČSOB		
CZ	Komerční Banka		
GR	NATIONAL BANK OF GREECE		
IT	BANCA SELLA		
NL	ABN AMRO		
RO	BANCA TRANSILVANIA		

3. Intermediaries

Overview of intermediaries:

Intermediary	Service name	App/ website/ both
Authologic		
itsme		
Mastercard		
Walt.id		
Lissi		
Bank ID		

Must be noted that, no specific Authentic Source was identified, that could be used in the context of PA1 for the issuance of TaxID / Certificate of Residence attestations. Therefore, these attestations will be issued by the Attestation Providers (e.g. IDnow) of PA1 as mock ones.

Regarding PIDs, the ones defined within the “PID & EBWOID Provider” group and relate to Czech Republic, Italy, Germany and Spain will be used. No additional PID providers were identified.

4.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	WALT.ID	CZ	
	ARICOMA	GR	
	LISSI	IT	
	COMPELLIO	NL	
	SAMSUNG	RO	
	IZERTIS	ES	
2. PID Provider	WP4 (PID & EBWOID Provider)	CZ DE ES IT	
3. Trusted list registrar	WP4 (Raidiam)		
4. Trust List or LoTE	WP4 (ID Union)		
5. QEAA provider	IDnow	DE	
	InfoCert	IT	
6. Pub-EAA provider			
7. EAA provider	BANKID	CZ	
	Mastercard		
8. QES provider			

4.3 Target country combinations

The targeted country combinations are the following:

		Issuing country			
		CZ	DE	ES	IT
Relying Party country	CZ		X	X	X
	GR	X	X	X	X
	IT	X	X	X	
	NL	X	X	X	X
	RO	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

The attestations to be used in this scenario, apart from PID, are:

- TaxID
- Certificate of Residence
- IBAN Ownership

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

The attestations will be used in the scenario, but will NOT be designed, implemented and issued to wallet within the scenario are:

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	This is the natural-person Person Identification Data (PID)	PID	CZ, DE, ES, IT	Issuable to WALT.ID Wallet and/or ARICOMA Wallet and/or LISSI Wallet and/or COMPELLIO Wallet and/or SAMSUNG Wallet and/or IZERTIS Wallet and/or WP4 provided wallets. The attribute “personal_administrative_number” and “portrait” should not be empty. PID must be valid (not revoked or expired) at the time of presentation. PID Provider must be registered in the Trust List provided by WP4. Must align with the We Build PID Rulebook

5.3 Created attestations in the scenario

Attestation name	Short description	For Countries	Applicable domain standards
TaxID	An attestation with the tax ID number of the natural person.	CZ, DE, ES, IT	
Certificate of Residence	An attestation with the recent residence address of the person (e.g. less than 3 months old)	CZ, DE, ES, IT,	
IBAN Ownership	An attestation stating that the specific person is the owner of a bank account in a different bank. Provided by the RP Bank (as EAA Provider) in scenario 4	CZ, DE, ES, IT	

Must be noted that, no specific Authentic Source was identified, that could be used in the context of PA1 for the issuance of TaxID / Certificate of Residence attestations. Therefore, these attestations will be issued by the Attestation Providers (e.g. IDnow) of PA1 as mock ones.

Regarding IBAN Ownership attestation, it is an attestation proving that a particular individual owns a bank account at a specific bank. This is important information, as it can facilitate the Due Diligence processes outlined in the Anti-Money Laundering Regulation (EU 2024/1624). However, it must be clarified that this attestation should not be mandatory, as a user may be attempting to open a bank account for the first time.

In scenario 1 we assume that a single user will attempt to open bank accounts with all available cross-border banks (RPs). Initially, this process will be performed using only the PID, TaxID and Certificate of Residence attestations. Once the first account is created and the corresponding IBAN Ownership attestation is issued to the user's wallet, the user will then proceed with the remaining banks, using all four attestations: PID, TaxID, Certificate of Residence and IBAN Ownership.

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 possess a valid EUDI Wallet instance
	b. MUST have a valid PID attestation issued by the respective Member State
	c. (MVP) MUST have a valid (Q)EAA for Residential Address, Tax ID
2. Authentic sources	a.
	b.
3. Relying party	a. MUST be able to directly integrate with EUDI Wallets to receive and evaluate TaxID, Certificate of Residence and IBAN Ownership attestations.
	b. MUST be able to issue IBAN Ownership attestations.
	c. MUST be registered as RP in the Member state Registrar provided by WP4, either themselves or via the Intermediary
	d. MUST obtain and manage the Access Certificate (e.g. X.509) from an Access Certificate Authority to authenticate toward the EUDI Wallets, if they opt in for direct integration
	e. SHOULD manage and present registration certificates (if issued), if they opt in for direct integration
	f. COULD use an Intermediary authorizing them to act on their behalf for attestation requests, with evidence of the relationship stored in the Member State Registrar
	g. MUST Define which attributes are required for KYC (e.g. PID, address, Tax ID)
	h. MUST integrate with the intermediary via REST APIs to trigger requests and receive verifiable claims, if they choose to be intermediated
	i. MUST verify the authenticity, integrity and validity of the PID and (Q)EAAs received from the EUDIW, by: a. Validating the Issuer's signature and certificate chain against the applicable Trusted List / LoTE b. Verifying that the issuer is authorised to issue the specific attestation type (e.g. via Trusted List, LoTE, or Rulebook-defined trust anchors). c. Verifying credential integrity by validating the issuer's signature on the credential d. Verifying holder binding by validating the proof-of-possession (PoP/device signature) to ensure the presenter controls the private key to which the credential is bound e. Checking credential status (revoked/suspended/valid) using Status Lists as defined by WP4
	j. MUST be interoperable with EUDI Wallets from Aricoma, Compellio, Izertis, Samsung, Walt.id, Lissi
4. Intermediary	a. MUST register in the Member State Registrar as a Service Provider, while indicating intentions to act as an intermediary
	b. MUST obtain and manage the Access Certificate (e.g. X.509) from an Access Certificate Authority to authenticate toward the EUDI Wallets
	c. MUST register each RP using their services in the Member State Registrar where the Relying party is established via a Registrar API, meaning that a single registration is sufficient for the MVP, but registration in multiple jurisdictions MUST be supported in later phases for cross-border scenarios.
	d. COULD receive one or more registration certificates for the intermediated RP, if the Registrar (via a Provider of registration certificates) issues registration certificates

	e. SHOULD manage and present registration certificates, if issued, on behalf of RPs for each intended use cases
	f. MUST include in the presentation request metadata about the RP and intended use case if no registration certificate is available such as: i. User-friendly name of the RP ii. Unique identifier of the RP iii. URL of the Registrar for the RP iv. Identifier of the intended use This extension is already supported in OpenID4VP 1.0.
	g. MUST verify the authenticity, integrity and validity of the PID and (Q)EAAs received from the EUDIW, by: a. Validating the Issuer's signature and certificate chain against the applicable Trusted List / LoTE b. Verifying that the issuer is authorised to issue the specific attestation type (e.g. via Trusted List, LoTE, or Rulebook-defined trust anchors). c. Verifying credential integrity by validating the issuer's signature on the credential d. Verifying holder binding by validating the proof-of-possession (PoP/device signature) to ensure the presenter controls the private key to which the credential is bound e. Checking credential status (revoked/suspended/valid) using Status Lists as defined by WP4
	h. MUST be interoperable with EUDI Wallets from Aricoma, Compellio, Izertis, Samsung, Walt.id, Lissi
	i. SHOULD maintain internal credential catalogues for PID, Certificate of address, Tax ID, IBAN, SCA, with defined schemas from WP4
	j. MUST validate that attestation payloads conform to the defined Attestation Rulebooks (schemas) for PID, Residential Address, Tax ID
	k. MUST normalize data attributes into a common API response format for the RP, including standardized error codes if verification fails
	l. MUST forward verified data to the RP only after successful checks, and MUST not forward any attributes to the RP if verification fails
	m. MUST NOT persist any PID or EAA attribute values (PII) to storage. MUST delete all user data after transmission to the RP. Logs MUST contain only verification metadata.
5. EUDI Wallet provider	a. MUST accept PIDs from CZ, DE, ES, IT
	b. MUST accept Attestations: i. TaxID ii. Certificate of Residence iii. IBAN Ownership
	c. MUST support receiving Presentation Requests via Cross-Device (QR Code) and Same-Device (Deep Link) flows
	d. COULD support DC API for presentation requests
	e. MUST Verify the RP / Intermediary's access certificate
	f. MUST provide explicit UX that displays the names of both the intermediary and the RP to the User when asking for consent, e.g. "Requestor: [Intermediary Name] on behalf of: [RP Name]", when RP is intermediated
	g. MUST verify the link between the Intermediary and the RP, by either: i. Validating the Registration Certificate included in the request, OR ii. Querying the Registrar API using the provided RP Identifier.
6. PID Provider	a. CZ, IT PIDs MUST be available
	b. PIDs MUST be issuable to provided partner wallets (AT, CZ, DE, LU, PL) and/or the ones to be provided by WP4
	c. "portrait" attribute MUST NOT be left empty
	d. "personal_administrative_number" attribute will be treated as the "national identification number" (AML Regulation) and therefore MUST NOT be left empty

7. Trust Infrastructure	a. Member State Registrar & Registrar API: to register RPs and Intermediaries when acting on behalf of RPs. The API MUST be available for Wallets to verify this relationship and to check for the RP's entitlements
	b. MUST issue Access certificates to the RPs and intermediaries
	c. MUST make available the trust anchors required for Wallets to validate access certificates for intermediaries/RPs
	d. COULD issue RP registration certificates via Provider(s) of registration certificates
	e. MUST support ETSI 119 612 and ETSI 119 602
	f. Status lists MUST be published by issuers so verifiers can check attestations have not been revoked
	g. MUST publish a Wallet Trust List to verify which Wallet Providers are valid, and that wallet providers in scenario 1 are listed in the Wallet Trust List
	h. Trusted Lists containing trust anchors MUST be published so verifiers can validate issuer trust chains and attestation signatures (authenticity/integrity), and status information to validate issuer authorisation (e.g. is this (Q)EAA provider allowed to issue this (Q)EAA?)
	i. COULD publish an attestation catalog to validate attestation scheme conformance
8. QEEA Provider	a. Since authentic sources are not available (e.g. TaxID, Certificate of Residence), IDnow MUST be able to create synthetic data or follow manual process.
	b. Attestations MUST be issuable to provided partner wallets (AT, CZ, DE, LU, PL) and/or the ones to be provided by WP4
9. Pub-EAA provider	a. N/A
	b.
	c.
10. EAA provider	a. N/A
	b.
	c.
11. QES provider	a. N/A
	b.
	c.

WE BUILD consortium

Specification WP3 PA1 – Contract- signing in banking KYC and onboarding of end-users

WP3 – PA1

Date : 2026-06-16
Version : 0.82(<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)
Status : Draft(Draft, for review, reviewed, final)

Index

1	Introduction	3
1.1	<i>Objectives of this document.....</i>	3
1.2	<i>Scenario introduction.....</i>	3
2	Scenario specification.....	3
2.1	<i>Introduction</i>	3
2.2	<i>Scenario pre-conditions</i>	4
2.2.1	<i>Two QES Implementation Models for WE BUILD PA1.....</i>	4
2.3	<i>Scenario main flow</i>	6
2.4	<i>Scenario additional flows.....</i>	7
2.5	<i>Challenges and barriers</i>	8
2.6	<i>Working Assumptions</i>	8
3	Detailed scenario flow.....	9
4	Roles and participants	11
4.1	<i>Scenario roles and participants.....</i>	11
4.2	<i>Additional roles and partners</i>	11
4.3	<i>Target country combinations.....</i>	12
4.4	<i>Requirements.....</i>	12
5	Electronic Attestations of Attributes (EAA)	13
5.1	<i>Introduction</i>	13
5.2	<i>Attestations to be provided by other UCs/WGs/scenarios.....</i>	13
5.3	<i>Created attestations in the scenario</i>	13
	Annex 1 – Requirements for scenario roles.....	15

1 Introduction

1.1 Objectives of this document

This document details the WE BUILD WP3 PA1 Scenario 3 — Contract Signing with Qualified Electronic Signatures (QES) using the EUDI Wallet. It outlines the technical, regulatory and organizational processes to be piloted cross-border, the attestations involved and the partners participating, in compliance with eIDAS 2.0 (Regulation (EU) 2024/1183) and aligned with the WE BUILD PA1 Stock Taking document v1.0 and the PA1 v0.7 evaluation.

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 pilots the cross-border signing of legally binding contracts by natural persons using QES via the EUDI Wallet, with legal equivalence to handwritten signatures across the EU. Two QES use cases are in scope: (i) signing the account-opening contract during onboarding (MVP), and (ii) signing of subsequent service contracts by existing customers (e.g. credit line, mortgage, card issuance, investment product) — MVP+. Only the Natural Person Wallet is in scope; Company Representative / Legal Person Wallet flows are out of scope for PA1.

The scenario is based on the following documentation:

- ARF v2.8.0 (<https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.8.0/architecture-and-reference-framework-main/>)
- ARF v2.8 Technical Specification 12 — SCA implementation with the wallet
- eIDAS 2.0 Regulation (EU) 2024/1183 — incl. Recital 62 and Article 5f(2) on SCA
- PSD2 (Directive (EU) 2015/2366); draft PSD3 / PSR proposals
- AMLR (EU) 2024/1624 (Anti-Money Laundering Regulation)
- ETSI EN 319 401 / 319 411 (general policy and certificate policy requirements for TSPs)
- ETSI TS 119 431-1 (TSP service components operating a remote QSCD)
- ETSI TS 119 432 / CSC API v2 (protocols for remote signature creation)
- W3C Verifiable Credentials Data Model; SD-JWT VC (IETF draft); OpenID4VCI 1.0; OpenID4VP 1.0; W3C Digital Credentials API
- WE BUILD PA1 Stock Taking v1.0; WE BUILD WP3 PA2 Stock Taking v1.01; WE BUILD Common Specifications (WBCS), ADRs and Trust Framework; EWC Implementation Guide v1.2

2 Scenario specification

2.1 Introduction

This scenario demonstrates cross-border contract signing by natural persons using the EUDI Wallet and QES, under WE BUILD WP3 PA1 Scenario 3. The QTSP-centric model is piloted as the MVP (primary), and the Wallet-centric model is piloted as MVP+ (secondary). Only the Natural Person Wallet is in scope. Two QES use cases are in scope: signing the account-

opening contract during onboarding (MVP) and signing a subsequent service contract by an existing customer (MVP+). Company Representative / Signing Rights mandate flows are explicitly out of scope for PA1.

2.2 Scenario pre-conditions

- The user holds a valid EUDI Wallet (Natural Person Wallet) with a PID in which the attributes 'portrait' and 'personal_administrative_number' are populated.
- The user holds a valid SCA-User attestation issued under PA1 Scenario 4; RP login for the QES initiation flow is performed using SCA-User.
- The Relying Party (bank) is registered, integrated with the wallet via OpenID4VP 1.0 and able to verify QES via trust lists.
- The QTSP (IDnow Trust Services AB) is integrated per ETSI TS 119 431-1 and ETSI TS 119 432 / CSC API v2 and aligned with ARF v2.8 TS12 where applicable.
- All technical components (wallet, RP, QTSP, trust lists) are interoperable per ARF v2.8.0 and WE BUILD WBCS/ADRs; trust list access is provided through the PA1 trust infrastructure (and intermediary, where applicable — see §4.2).

2.2.1 Two QES Implementation Models for WE BUILD PA1

According to the EUDI Wallet architecture, there are two main models for implementing Qualified Electronic Signatures as part of the European Digital Identity Wallet (EUDI Wallet) for business and payment use cases, specifically needed for use case 3 (Sign a contract):

2.2.1.1 QTSP-Centric Model (Primary/MVP QES model due to PA1 survey / Wallet-Triggered)

In this model, the wallet triggers and authorizes a remote signing service, but the actual signature is created by a QTSP on behalf of the user.

Key Characteristics:

- The QTSP operates a Remote QSCD
- The wallet is used to authenticate and authorize the signing request
- The QTSP creates the signature based on wallet authorization
- The wallet presents credentials and confirms transaction data

Exemplary Use Cases:

a) Complex Multi-Party Contract Signing

- Opening a joint account or business account with multiple signatories
- Bank uploads contract to QTSP remote signing platform
- Each authorized party receives signing request in their EUDI Wallet
- Wallet authenticates user and presents transaction data for approval
- User authorizes QTSP to sign on their behalf
- QTSP creates QES and applies it to the document
- Benefits: Better suited for complex workflows, audit trails, sequential signing

b) High-Value Transaction Authorization

- For significant financial commitments (mortgage applications, investment accounts)
- Bank requires qualified signature with additional assurance
- Wallet triggers remote signing with strong authentication
- QTSP provides additional security layers and comprehensive audit logs
- Signature includes qualified timestamp and long-term validation data

2.2.1.2 *Wallet-Centric Model (Secondary/MVP+ QES model due to PA1 survey)*

In this model, the signature is created inside the wallet itself, with support from a QTSP for the cryptographic signature value.

Key Characteristics:

- The EUDI Wallet acts as or contains a Qualified Signature Creation Device (QSCD)
- The private signing key is protected within the wallet's secure element (or alternatively, a smart card with NFC could be used as local QSCD)
- The wallet directly creates the signed document or just the signature
- The QTSP provides supporting services (certificate issuance, timestamp services)

Exemplary Use Cases:

a) Account Opening Contract Signing

- Customer completes bank account application via mobile/web
- Bank sends the account opening contract to the customer's EUDI Wallet
- Customer reviews terms and conditions directly in the wallet interface
- Customer authenticates using wallet's authentication
- Wallet generates QES using its internal QSCD
- Signed contract is returned to the bank immediately
- Benefits: Instant signature, no external service dependency, enhanced privacy

b) Credit Agreement Signing

- When opening a credit line or loan account
- Wallet presents transaction data (loan amount, interest rate, terms)
- Customer reviews and confirms transaction data in the wallet
- QES is created with cryptographic binding to transaction data
- Provides non-repudiation for high-value financial commitments

2.2.1.3 *Hybrid model*

Exemplary Hybrid Use Cases (Combining Both Models):

a) Tiered Product Onboarding

- Basic account opening: wallet-centric QES for speed
- Premium services (investment, wealth management): QTSP-centric for enhanced audit

b) Compliance Documentation

- Self-declaration forms: signed in wallet

- Notarized or witnessed documents: signed via QTSP with additional attestations

2.2.1.4 Technical Integration Points

Both models use OpenID4VP (OpenID for Verifiable Presentations) authorization requests to interact with the wallet:

1. Relying Party (Bank) sends signing request
2. Wallet presents required credentials (PID, QES certificate)
3. Transaction data (document hash, signing details) is confirmed
4. QES is created (either in wallet or by QTSP)
5. Signed document is returned to bank

2.2.1.5 Summary

In WE BUILD PA1, both QES models may play complementary roles:

- QTSP-centric (primary) QES is better for complex workflows, long-term archival, and enhanced audit requirements
- Wallet-centric (secondary) QES is ideal for straightforward, immediate signature needs during onboarding

The choice depends on the specific onboarding scenario, regulatory requirements, and the level of assurance needed for the signed documents. However, PA1 survey the MVP model with be the QTSP-centric one.

2.3 Scenario main flow

Swim Lane Diagram (textual)

Step	User (Wallet)	Relying Party	Intermediary	(Q)EAA Provider	QES Provider	(L)PID Provider
1	Initiates contract signing	Presents contract	(optional)	-	-	-
2	Authenticates & consents	Requests QES	(optional)	-	-	-
3	Authorizes QES in wallet	Receives signed contract	(optional)	-	Creates QES	-
4	Receives confirmation	Stores QES	(optional)	-	-	-

Main Steps:

1. User logs in to the RP portal using the SCA-User attestation (issued in Scenario 4) and selects 'Sign with EUDI Wallet'.
2. RP presents the contract and sends an OpenID4VP 1.0 Authorization Request (same-device deeplink or cross-device QR) containing the document hash / transaction data.
3. User authenticates to the wallet (PIN / biometric); the wallet validates the Authorization Request and presents the contract for review under the 'what you see is what you sign' (WYSIWYS) principle. The wallet displays the human-readable

contract content (or a wallet-rendered preview of the document) together with the signed transaction data — signer, RP, signing purpose, timestamp and the document hash — and recomputes the hash over the displayed document to confirm it matches the hash in the request before the user authorises the QES.

4. User consents. In the QTSP-centric model (MVP) the wallet authenticates the user to IDnow Trust Services AB per CSC API v2; in the Wallet-centric model (MVP+) the wallet uses its local QSCD.
5. The QES is created and applied to the document (hash-signing as the primary integration pattern; PDF signing optional).
6. Signed contract is returned to the RP; RP verifies the QES against EU trust lists and archives the signed document.

2.4 Scenario additional flows

Flow	Short Description	Variations	Exceptions
Basic same-device	User initiates and signs on the same device via deeplink (OpenID4VP).	—	User declines consent (access_denied)
Basic cross-device	User initiates on PC and signs on mobile via QR (OpenID4VP).	Device handover	Cross-device session timeout
Wallet-centric QES (MVP+)	Signature created inside the wallet using its local QSCD.	Same/cross-device	Wallet does not support local QSCD → fallback to QTSP-centric
QTSP unavailable	QTSP service outage during signing.	Retry / alternative QTSP	QES issuance error
SCA-User missing/revoked	User cannot log in to RP because SCA-User is invalid.	Re-issuance via Scenario 4	Process terminates
QES certificate revoked	User's QES certificate is revoked at signing time.	—	RP terminates the flow

Out of scope (not piloted): Legal Person Wallet, multi-signature/sequential signing, Advanced Electronic Signatures (AES), and Company Representative / Signing Rights mandate flows.

Flow	Short description
Variations	
-	
-	
Exceptions	

-	
-	
-	
-	

2.5 Challenges and barriers

- Technical: evolving ARF profiles and OpenID4VP/4VCI versioning; conformance to CSC API v2 (ETSI TS 119 432) for QTSP integration; availability of QSCD-capable wallets for the Wallet-centric model (MVP+); trust list mechanisms covering both issuer and QTSP trust.
- Regulatory: national differences in contract law; cross-border QES recognition under eIDAS Art. 25; AMLR (2024/1624) onboarding requirements; GDPR proportionality of attribute disclosure.
- Organizational: dependency on PA1 Scenario 4 (SCA-User issuance) and on the PA1 trust infrastructure; alignment with RPs across CZ, GR, IT (and additional PA1 countries) and with wallet providers.
- Commercial: cost and onboarding lead time for QTSP services; sustainable business model for QES issuance; user adoption of wallet-driven signing flows.

2.6 Working Assumptions

- ARF v2.8 (incl. TS12) and the related eIDAS 2.0 implementing acts are stable by pilot launch.
- IDnow Trust Services AB provides a remote QSCD (QTSP-centric, MVP); a subset of wallet providers will support QSCD-based wallet-centric QES (MVP+).
- EU trust lists are available and accessible cross-border for QES validation; document hash signing is the primary integration pattern (full PDF signing optional).

3 Detailed scenario flow

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

Step	Actor	Action	Dependencies	Variations/Exceptions
1	User	Logs in to RP portal using SCA-User attestation (issued in Scenario 4); selects 'Sign with EUDI Wallet'.	SCA-User attestation (Scenario 4), RP portal	SCA-User missing/revoked → re-issuance via Scenario 4
2	Relying Party	Presents contract; creates OpenID4VP 1.0 Authorization Request with document hash / transaction data; same-device deeplink or cross-device QR.	OpenID4VP 1.0, WBCS	Cross-device handover; session timeout
3	User / Wallet	User authenticates to the wallet; the wallet validates the Authorization Request and applies the WYSIWYS principle: it renders the contract (human-readable content / document preview) and the transaction data, recomputes and matches the document hash, and obtains the user's review before authorisation.	PID, wallet authentication	Authentication failure; user declines (access_denied)
4	Wallet ↔ QTSP	QTSP-centric (MVP): wallet authenticates user to IDnow Trust Services AB and authorises remote signing per ETSI TS 119 432 / CSC API v2. Wallet-centric (MVP+): wallet uses local QSCD.	QTSP integration (CSC API v2, ETSI TS 119 431-1), QES certificate	QTSP unavailable; QSCD unavailable in wallet
5	QTSP / Wallet	QES is created (hash-signing primary; PDF signing optional) and	Remote QSCD or local QSCD	QES issuance error

		applied to the document; qualified timestamp added.		
6	Wallet	Returns signed document (or detached signature) to RP via OpenID4VP response.	OpenID4VP response	Transport error
7	Relying Party	Verifies QES against EU trust lists; stores signed contract; confirms to user.	EU trust list, RP archive	QES invalid; certificate revoked

Main flow step – same-device website to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
... Step name	... Swimming lane name	... Detail per action (chronologically) what happens in this step. Use 1 row per action.	... Declare any attestations or items to be provided by other UCs for this action. This must be in line with section 3 of the Stock Taking document.	... In case variations/ exceptions have been declared in the previous section, they can be mentioned here if applicable for the activity.
		... Detail per action (chronologically) what happens in this step. Use 1 row per action.	... Declare any attestations or items to be provided by other UCs for this action. This must be in line with section 3 of the Stock Taking document.	... In case variations/ exceptions have been declared in the previous section, they can be mentioned here if applicable for the activity.
		... Detail per action (chronologically) what happens in this step. Use 1 row per action.	... Declare any attestations or items to be provided by other UCs for this action. This must be in line with section 3 of the Stock Taking document.	... In case variations/ exceptions have been declared in the previous section, they can be mentioned here if applicable for the activity.

4 Roles and participants

4.1 Scenario roles and participants

Primary Role	UC Partner Name	Country
User of EUDI Wallet	Natural person end-user (pilot tester)	CZ, GR, IT, NL, RO
Authentic Sources	Per-country PID issuers (national PID providers under WP4/PA3)	Per pilot country
Relying Party	NATIONAL BANK OF GREECE; BANCA SELLA	GR; IT
Intermediary	Not used in Scenario 3 (direct RP–Wallet integration). To be revisited if a PA1 intermediary is introduced.	—

Primary role	UC partner Name	Country
1. User of EUDI Wallet		
2. Authentic sources		
3. Relying party	Add the name of the organization, the name of the service provided and the name of the portal	
4. Intermediary		

4.2 Additional roles and partners

Primary Role	UC Partner Name	Country
Wallet Provider	WALT.ID (with NBG); IZERTIS (with Banca Sella). Other PA1 wallets (ARICOMA, COMPELLIO, LISSI, SAMSUNG) usable if RPs extend Scenario 3 coverage.	AT; ES (others: CZ/DE/PL)
PID Provider	Per-country PID issuers (under WP4/PA3)	Per pilot country
Trusted List Registrar	National supervisory bodies maintaining EU trust lists	Per MS
QEAA Provider	IDnow Trust Services AB	SE
QES Provider	IDnow Trust Services AB (sole QTSP for Scenario 3)	SE

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider			
2. PID Provider			
3. Trusted list registrar			
4. QEAA provider			
5. Pub-EAA provider			
6. EAA provider			
7. QES provider			

4.3 Target country combinations

PID Issuing Country	Relying Party Country
CZ	GR, IT
IT	GR, IT
GR	GR, IT

	Issuing country						
Relying Party country		AT	BE	DE	FI	FR	...
	AT						
	BE						
	DE						
	FI						
	FR						
	...						

4.4 Requirements

5 Electronic Attestations of Attributes (EAA)

5.1 Introduction

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

Attestation name	Short description	To be provided by	For Countries	Requirements
PID	Natural-person Person Identification Data (PID) used to identify the signatory and bind the QES certificate to the natural person.	WP4 / national PID providers (PA3)	GR, IT (and other PA1 countries where Scenario 3 is extended)	Issuable to WALT.ID Wallet (NBG flow) and IZERTIS Wallet (Banca Sella flow), and to other PA1 wallets where applicable. The attributes 'personal_administrative_number' and 'portrait' SHALL NOT be empty. Compliant with eIDAS 2.0 and ARF v2.8 PID rulebook.
SCA-User	Strong Customer Authentication attestation used by the user to authenticate to the RP portal before initiating the QES flow.	PA1 Scenario 4	All Scenario 3 pilot countries	eIDAS 2.0 Art. 5f(2) and Recital 62; PSD2/PSR; ARF v2.8 TS12; WE BUILD SCA Attestation Rulebook.

Attestation name	Short description	To be provided by	For Countries	Requirements

5.3 Created attestations in the scenario

-

Attestation name	Short description	For Countries	Applicable domain standards
QES Certificate (short-term qualified certificate for electronic signature)	Qualified certificate bound to the natural person and to the wallet, used to create the QES on the contract. In the QTSP-centric model the corresponding private key is held in a remote QSCD operated by the QTSP; in the Wallet-centric model (MVP+) the key is held in a local QSCD within the wallet.	SE (issued by IDnow Trust Services AB; usable cross-border for RPs in GR and IT, and others where Scenario 3 is extended)	eIDAS 2.0 (Regulation (EU) 2024/1183); ETSI EN 319 401; ETSI EN 319 411-2 (QCP-n-qscd); ETSI EN 319 412-2 and 412-5; ETSI TS 119 431-1 (TSP operating a remote QSCD); ETSI TS 119 432 / CSC API v2; ARF v2.8 incl. TS12; OpenID4VP 1.0; SD-JWT VC.
QES (qualified electronic signature on the contract)	The QES applied to the contract document (hash-signing as the primary integration pattern; full PDF signing optional). Includes a qualified electronic timestamp.	SE (signature creation by IDnow Trust Services AB); verifiable by any RP in the EU via trust lists	eIDAS 2.0 Art. 25/26; ETSI EN 319 122 / 319 132 / 319 142 (AdES formats: CAdES/XAdES/PAdES); ETSI EN 319 422 (qualified timestamps); EU Trust List (LOTL).

Annex 1 – Requirements for scenario roles

Primary role	Specific requirement
1. User of EUDI Wallet	a. TBD
	b. TBD
	c. TBD
2. Authentic sources	a. No additional authentic-source attestations are required for the signing process. Only PID (from PID Providers) and the SCA-User attestation (from Scenario 4) are used. - i. - ii. - iii. - iv. - v. - vi.
	b. N/A for Scenario 3 (no optional attestations consumed in the signing flow).
	c. Synthetic data may be used for PID where no authentic source is available for a pilot country.
	d. N/A
3. Relying Party	a. NATIONAL BANK OF GREECE
	b. BANCA SELLA
4. Intermediary	c. N/A
5. EUDI Wallet provider	b. Accept PIDs from: WALT.ID (with NBG, AT) IZERTIS (with Banca Sella, ES) Other PA1 wallets (ARICOMA, COMPELLIO, LISSI, SAMSUNG) usable if Scenario 3 RP coverage is extended.
	c. Accept attestations: - PID (mandatory) - SCA-User attestation (from Scenario 4, for RP login) - QES certificate (issued by IDnow Trust Services AB)
6. PID Provider	a. GR and IT PIDs must be available for Scenario 3 RPs (NBG, Banca Sella).
	b. GR PID issuable by WALT.ID Wallet (NBG flow); IT PID issuable by IZERTIS Wallet (Banca Sella flow).
	c. PID <u>must</u> include: family_name, given_name, birth_date, birth_place, nationality (or statelessness, refugee, or subsidiary protection); PID <u>shall</u> include: personal_administrative_number (where available), resident_country, resident_state, resident_city, resident_postal_code, resident_street, resident_house_number, resident_address;
7. Trusted list registrar	a. TBD
	b. TBD
	c. TBD
8. QEAA provider	d. IDnow Trust Services AB (SE) certified and able to issue the QES certificate and, where applicable, support SCA-User issuance for the signing flow.

	b. N/A (no contract-specific QEAs are consumed in the signing process).
9. Pub-EAA provider	a. N/A
	b. N/A
	c. N/A
10. EAA provider	a. N/A
	b. N/A
	c. N/A
11. QES provider	a. Provision of short-term QES certificates for contract-signing by IDnow Trust Services AB (SE), per ETSI EN 319 411-2 / 319 412-2/-5, ETSI TS 119 431-1, ETSI TS 119 432 / CSC API v2.
	b. Operational model support: - QTSP-centric (MVP, primary): remote QSCD operated by IDnow Trust Services AB - Wallet-centric (MVP+, secondary): local QSCD within wallet, where supported
	c. Hash-signing is the primary integration pattern; full PDF signing is optional and depends on RP/wallet capability.

WE BUILD consortium

Specification Scenario 4 – Issue Attestations and Micro-credentials to the Wallet

WP2 – Use Case [PA1]
Consumer Banking

Date : 15.1.2025
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 specification	3
2.1	<i>Introduction</i>	<i>3</i>
2.2	<i>Scenario pre-conditions</i>	<i>4</i>
2.3	<i>Scenario main flow</i>	<i>4</i>
2.4	<i>Scenario additional flows</i>	<i>4</i>
2.5	<i>Challenges and barriers.....</i>	<i>5</i>
2.6	<i>Working Assumptions.....</i>	<i>5</i>
3	Detailed scenario flow	6
4	Roles and participants.....	10
4.1	<i>Scenario roles and participants</i>	<i>10</i>
4.2	<i>Additional roles and partners</i>	<i>10</i>
4.3	<i>Target country combinations</i>	<i>10</i>
4.4	<i>Requirements</i>	<i>10</i>
5	Attestations	11
5.1	<i>Introduction</i>	<i>11</i>
5.2	<i>Attestations to be provided by other UCs/WGs/scenarios</i>	<i>11</i>
5.3	<i>Created attestations in the scenario.....</i>	<i>11</i>
	Annex 1 – Requirements for scenario roles	12

1 Introduction

1.1 Objectives of this document

This document describes detail of scenario 4 in use case PA1 in work package WP3 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

Scenario will focus on issuing banking attestation:

- SCA-User
- SCA -IBAN
- IBAN ownership (IBAN-OV)

To users with active Wallet.

The scenario is based on the following documentation:

1. ARF in current version (2.9.0)
2. SUA Attestation specification in EUDIW Standards and Technical specifications TS12
3. OpenID for Verifiable Credential Issuance 1.0 optionally 1.1
4. WP4 Architecture Credential Issuance specification
5. ETSI for authentic source interfaces
6. ETSI TS 119 472 part 1 and 3

2 Scenario specification

2.1 Introduction

After the digital onboarding process the customers usually require an attestation in their wallets that can confirm the bank account number, and the Strong Customer Authentication means so that they can use the banking services in the banking portal or the bank mobile application. This scenario aims to cover this User's need.

Attestations than can be used to:

- Authentication to bank (must be the same bank that issued the SCA)
- Confirmation of action requiring strong authentication in bank (must be the same bank that issued the SCA)
- Initiating payments
- Confirmation of account ownership/control (owner/mandate ..)

Detail usage of such attestations in described in TS12 technical standard published by European Committee on GitHub. Also usage of SCA credentials is piloted in use case PA2.

Flows and sequence diagrams are available at WP3 Technology&Standards group GitHub in folder of PA1 here

<https://github.com/webuild-consortium/wp3-technology-standards/tree/main/sequence-diagrams/PA1/Scenario%204%20-%20Issue%20Credentials%20to%20Wallet>

UX flow is in Miro

<https://miro.com/app/board/uXjVJp-hKYY=/>

Password is shared on request

2.2 Scenario pre-conditions

Bank has sufficient data to match user, or bank has matched user based on PID.

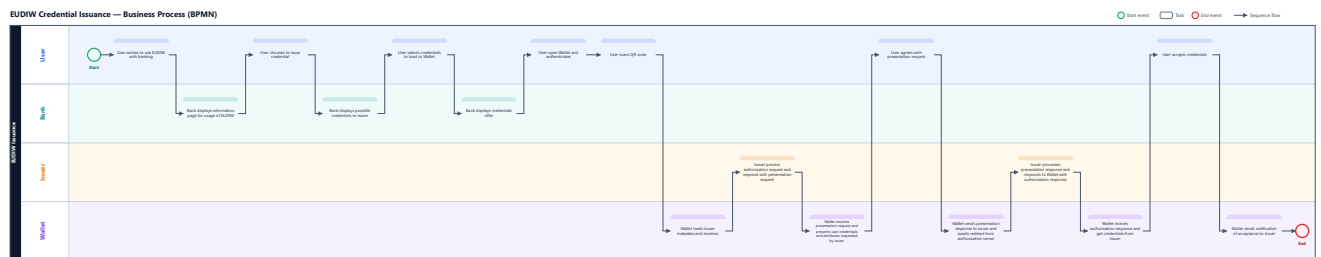
For IBAN Ownership user has at least one account as owner or joint account holder or authorized person.

User may be already authenticated in bank. User may have already presented PID to bank.

2.3 Scenario main flow

Flow may be direct continuation of on-boarding scenarios 1 and 2 but may also be initiated by current bank customer.

Main flow is described here with activity diagram.



2.4 Scenario additional flows

Scenario may have following main deviations

- usage of dedicated EAA issuer
- issuing on behalf of owner i.e. IBAN for child account

Flow	Short description	Is MVP
Variations		
- Usage of dedicated EAA/ issuer	Depending of bank's choice, Bank may split its role between itself as Authentic source and other party acting as EAA issuer providing Wallet interface part for issuance	Yes
- Revocation of credential after issuance	Bank or issuer may revoke credentials after issuance for various reasons	Yes
- Renew of credential	Wallet may request credentials renewal before expiry of credential	Yes
Exceptions		

- No valid attestation	User does not have SUA or PID for matching	
- No valid Wallet instance	User does not have valid Wallet instance	
- Issued credentials in not valid	Issued credentials may not have fulfilled conditions for SUA i.e. metadata are not properly published or have changed in time of issuance	
-		

In MVP we do not expect to implement issuing on behalf for example issuing to authorized person with usage of Power of attorney.

In MVP usage on dedicated issuer is one of possible implementation path as bank partners may not be interested in developing their own issuer.

2.5 Challenges and barriers

Industry standardization of the SCA-User and SCA-IBAN Attestation: No agreed EU-wide schema or rulebook for an IBAN attestation currently exists under eIDAS2/ARF. Piloting requires scenario partners to define and align on a fit-for-pilot attestation format, which may need revision as ARF guidance matures. Coordination with WP4 SEMANTICS is essential.

Immaturity and Instability of Payment Technical Specifications (TS12): The Technical Specification covering payments (TS12) is still not finalized and is expected to evolve significantly during the pilot development period. There is a risk that key design decisions made in this scenario — such as the SUA and SCA attestation format and its metadata, or the wallet invocation mechanism — may need to be substantially revised or even redesigned if TS12 undergoes major changes. This creates uncertainty for scenario partners investing in development ahead of specification stability, and close monitoring of TS12 progress will be required throughout the project lifecycle.

2.6 Working Assumptions

We assume following preconditions and assumptions to be true for implementation of this flows:

- Scenario assumes leveraging current bank partner account ownership and control schemes, no changes shall be required for issuing such credentials
- Scenario assumes that bank partners and issuer will use IBAN formats for accounts even if nationally other format used
- Scenario will not be making changes to current authentication and authorization schemes used by bank – this is scope of PA2 A.1 scenario
- Scenario assumes that participating Wallets for issuance will need minimal changes. Changes required for implementation of TS12 should be done in PA2 A.1/2 scenarios

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
User wishes to use EUDIW with banking	User	In banking website or application user chooses to binding his EUDIW and use it for login and/or payment		
Bank displays information page for usage of EUDIW	Bank	In banking website or application bank displays information (page or overlay) about connecting EUDIW to bank with possibility to initiate credential issuance		Bank may skip this page/overlay and directly go to credential offer
User chooses to issue credential	User	User clicks on button		
Bank displays possible credentials to issuer	Bank	In bank application bank will list credentials that user may choose to issue to their Wallet. Bank will display at least SCA-User (under friendly name) and may display additional one like accounts and cards		Bank may also skip this page and offer user pre-selected credential set. May be combine with skipping information screen
User selects credentials to load to Wallet	User	In bank application user selects credentials that their wants to load to Wallet		
Bank displays credentials offer	Bank	In banking website or application bank displays credential offer QR code for credential offer with deep link from Wallet		If platform support DC API with issuance bank may send DC API request for issuance. Then DC API flow is used.

				- If offer should be displayed in application and bank doesn't support DC API, application may try initiating deep link via custom URI scheme
User open Wallet and authenticates	User	User open Wallet or platform open Wallet via system dialog and User authenticates to Wallet via biometric or pin code.	Wallets from use case and WP4 Wallet provider group	If DC API used DC API dialog in platform is used.
User scans QR code	User	User scans QR code	Wallets from use case and WP4 Wallet provider group	Step is omitted for DC API and deep link
Wallet loads issuer metadata and resolves	Wallet	Wallet loads credential issuer metadata, authorization server metadata and resolves pushed authorization request to authorization server.	Wallets from use case and WP4 Wallet provider group	
Issuer process authorization request and respond with presentation request	Issuer	Issuer process pushed authorization request from Wallet and responds with deep-link/DC API request for presentation		
Wallet resolves presentation request and presents user credentials and attributes requested by issuer	Wallet	Wallet performs several background flows picks up presentation request from issuer gets data for request from issuer present users credentials and attributes that issuer		DC API dialog may be used User may not have credential required by issuer

		needs for issuance of bank credentials		
User agrees with presentation request	User	User confirms in Wallet		If DC API is used User may confirm in DC API dialog
Wallet sends presentation response to issuer and awaits redirect from authorization server	Wallet	Wallet send presentation response to Issuer and returns to issuance flow awaiting authorization response from Issuer's authorization server		
Issuer processes presentation response and responds to Wallet with authorization response	Issuer	Issuer receives presentation response from Wallet, validates response and data and prepares authorization response that sends to Wallet via authorization server		Issuer may not accept data from wallet and will send error response
Wallet receives authorization response and get credentials from Issuer	Wallet	In this step there is multi-step technical interaction between Wallet and Issuer with following steps Wallet uses code from response to get tokens from Issuer's authorization server. Uses sender's constrained token via DPoP. Issuer returns access token and refresh token Wallet uses access token from previous to call credential endpoint for each credential		

		configuration and data set for it from Issuer. Sends proofs for credential binding and DPoP token. Issuer responds with one or more credentials of same type and data set for one requests. Once all credentials are obtained, Wallet displays list of credentials obtained to User		
User accepts credentials	User	User accepts credentials in wallet		
Wallet sends notification of acceptance to issuer	Wallet	Wallet sends acceptance notification of credentials		User may decline, Wallet then send rejecting notification and issuer will revoke invalidated credentials

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. Banks	NATIONAL BANK OF GREECE	GR
	BANCA SELLA	IT
	BANCA TRANSILVANIA	RO
	Air Banka	CZ
	Komerční Banka	CZ
	ČSOB	CZ
2. EAA issuers	BANK ID CZ	CZ
	MASTERCARD	BE

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. EUDI Wallet provider	LISSI	DE	
	COMPELLIO	LU	
	SAMSUNG	PL	
	ARICOMA	CZ	RW
	IZERTIS	BE	
2.			

4.3 Target country combinations

		Issuing country			
Wallet country		GR	IT	RO	CZ
	PL				X
	BE		X		X
	DE			X	X
	LU	X			X
	CZ				X

4.4 Requirements

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

5 Attestations

5.1 Introduction

This scenario requires only PID attestation and optionally for production ready flow WUA.

We assume that these attestations will be provided by partners within use case and WP4 Wallet group

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

Attestation name	Short description	To be provided by	For Countries	Requirements
WUA	Wallet Unit attestation	WP4 Wallet Group		
PID	PID attestation as per ARF requirements	PID providers in Use Case	CZ	
SCA-User	Strong user authentication attestation for login and confirmation of risk transaction used only by issuing bank	WP3 T&S Group	CZ	
SCA- IBAN	Strong user authentication attestation for login and confirmation of risk transaction and PISP payment initiation used by issuing bank and PISP to initiate payment	WP3 T&S Group	CZ	

5.3 Created attestations in the scenario

...

Attestation name	Short description	For Countries	Applicable domain standards
SCA-User	Strong User Attestation as per EDUIW Standard and Technical specification , TS12, used in PA2 A.1 and B.1	CZ, GR, IT, RO	Payments
SCA-IBAN	Strong User Attestation with IBAN as per EDUIW Standard and Technical specification , TS12, used in PA2 A.2	CZ, GR, IT, RO	Payments
IBAN Ownership	IBAN Ownership Attestation as confirmation of control of account	CZ, GR, IT, RO	

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario. Requirements in this list are only scenario specific requirements.

Primary role	Specific requirement
1. User of EUDI Wallet	a. No specific requirements
	b.
	c.
2. Authentic sources	a. Bank as authentic source can issue multiple identifiers for user for issuance of SUA
	b.
	c.
3. Relying party	a. Bank as relying party should accept only its own SUA attestation for authentication (SCA-user)
	b.
	c.
4. Intermediary	a. No scenario specific requirements
	b.
	c.
5. EUDI Wallet provider	a. No extra requirements than WP4 requirements and TS12 in EUDIW Standards and technical specifications
	b.
	c.
6. PID Provider	a. No scenario specific requirements
	b.
	c.
7. Trusted list registrar	a. No scenario specific requirements
	b.
	c.
8. EAA provider	a. Issued attestation shall be issued in SD-JWT and may be issued in mDoc format
	b. Issued SCA attestation must be device bound
	c. Issued attestation must support selective disclosure
	d. Issuance protocol used is Openid4VCI with HAIP in WP4 Architecture profile
	e. Issuance should support both issuing flows (authorized and pre-authorized code)
	f. Credentials may be issued in batches for production ready flow
	g. Issuer should request WUA as part of authorization request for production ready flows

	h. Issuer must publish metadata endpoints with respect to SD-JWT VC specification and extension by TS12 in EUDIW Standards and technical specifications
	i. SD-JWT metadata must extend SD-JWT metadata specified by this specification. This metadata will be published on public access URL

WE BUILD consortium

Specification Scenario 5 – Update the Originally Provided KYC

WPX – UC PA1

Date : 13 July 2026
Version : 1(<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)
Status : **reviewed** (Draft, for review, reviewed, final)

Index

1	Introduction	5
1.1	Objectives of this document.....	5
1.2	Scenario introduction.....	5
2	Scenario specification.....	6
2.1	Introduction	6
2.1.1	Use Case and MVP Scope.....	6
2.1.2	Wallet type.....	6
2.2	Scenario pre-conditions	6
2.2.1	Wallet and PID	6
2.2.2	Prior customer relationship	6
2.2.3	Session-level SCA capability	7
2.2.4	Place of Residence attestation issuance capability	7
2.2.5	Technical infrastructure	7
2.2.6	Standardisation baseline.....	7
2.3	Main flow.....	7
2.3.1	Steps 1-2: Trigger and notification	7
2.3.2	Step 3: Access to the online banking	7
2.3.3	Steps 4-5: Session SCA Authentication (MANDATORY).....	7
2.3.4	Step 6: Bank requests Place of Residence attestation	8
2.3.5	Steps 7-8: Attestation availability check; issuance if needed.....	8
2.3.6	Step 9: Presentation with consent	8
2.3.7	Step 10: Authorise data change with SCA (MANDATORY).....	8
2.3.8	Step 11: Verify attestation and update internal systems.....	9
2.3.9	Step 12: Confirmation	9
2.3.10	Swimlane diagram.....	9
2.4	Scenario additional flows.....	9
2.5	Challenges and barriers	10
2.5.1	Absence of operational Authentic Sources for residence	10
2.5.2	Consistency with the PA3 banking position on root of trust	10
2.5.3	Attestation freshness and bank CDD policy	11
2.5.4	Unstable and evolving standards	11
2.5.5	Interoperability	11
2.5.6	Banking system integration.....	11
2.5.7	Dependency on Scenario 4	11
2.5.8	Trust infrastructure maturity	11
2.6	Working Assumptions	11
2.6.1	SCA architecture and data-change authorisation	11
2.6.2	Validity period of the Place of Residence attestation	12
2.6.3	QTSP-issued synthetic attestation as pilot workaround	12
2.6.4	Versions and protocols	12
2.6.5	Selective disclosure	12
2.6.6	Trust registry and revocation	13
2.6.7	Same-device and cross-device	13
2.6.8	Role of the intermediary	13
2.6.9	CRM and core banking update.....	13
2.6.10	Periodic review triggers.....	13
2.6.11	Natural Person Wallet only	13
2.6.12	Partner commitment.....	13
2.6.13	Review process.....	13

3	Detailed scenario flow.....	14
3.1	<i>Phase 1: Trigger and access.....</i>	14
3.2	<i>Phase 2: Session-level SCA Authentication.....</i>	14
3.3	<i>Phase 3: Bank requests Place of Residence attestation.....</i>	14
3.4	<i>Phase 4: Attestation availability check and issuance.....</i>	14
3.5	<i>Phase 5: Presentation with consent and submission.....</i>	14
3.6	<i>Phase 6: Step 10 SCA and verification.....</i>	15
3.7	<i>Phase 7: Update of internal systems.....</i>	15
3.8	<i>Phase 8: Confirmation.....</i>	15
3.9	<i>Summary table.....</i>	15
4	Roles and participants.....	17
4.1	<i>Scenario roles and committed partners.....</i>	17
4.2	<i>Additional roles and ecosystem partners.....</i>	17
4.3	<i>Requirements.....</i>	17
5	Attestations	18
5.1	<i>Introduction</i>	18
5.2	<i>Attestations consumed but produced by other scenarios or WGs</i>	18
5.2.1	<i>Created attestations overview</i>	18
5.3	<i>Place of Residence attestation.....</i>	19
6	Annex 1 - Requirements for scenario roles	20
6.1	<i>User of EUDI Wallet</i>	20
6.2	<i>Relying Party (Bank).....</i>	20
6.3	<i>QTSP (Place of Residence issuer).....</i>	21
6.4	<i>EUDI Wallet Provider</i>	22
6.5	<i>Key dependencies.....</i>	23
7	Annex 2 - Glossary.....	24

Change log vs. v0.7

- Scope reduced: MVP now focuses on Place of Residence update only. Tax ID removed (covered by PID). Annual Income and Occupation moved to MVP+ and excluded from the MVP flow.
- SCA architecture: the position consolidated by the PA1 partner meeting of 26 March 2026 is reaffirmed. SCA at Step 10 (data-change authorisation) with transaction-specific binding remains the pilot default, on the normative basis of PSD2 Art. 97, RTS Art. 26 and PSR Art. 85. The mechanism for session-level SCA at Steps 4-5 is being analysed in Scenario 4; Scenario 5 will adopt whatever Scenario 4 produces. UX implementation (DC API vs deep link/app-switch) to be evaluated.
- Issuance approach for the pilot: Place of Residence attestation issued by a QTSP (InfoCert for IT, IDnow for DE/GR) as a synthetic attestation, in absence of operational Authentic Sources. Pilot workaround, explicitly documented.
- Dependency on Scenario 4 made explicit: the session-level SCA mechanism at Steps 4-5 is being analysed in Scenario 4. Scenario 5 fallback is the existing bank SCA method.
- Working Assumptions updated and consolidated to reflect the new MVP scope. Working Assumption 2.6.1 reaffirms SCA at Step 10 as confirmed by the PA1 partner meeting of 26 March 2026, with the session-level SCA mechanism deferred to Scenario 4.
- Roles and partners updated: InfoCert added as QTSP partner for Italian pilot; IDnow remains as QTSP for DE/GR.

1 Introduction

1.1 Objectives of this document

This document describes Scenario 5 of the Consumer Banking use case (PA1) within Work Package 3 of the WE BUILD consortium. Scenario 5 covers the update of Customer Due Diligence (CDD) information through the EUDI Wallet for a customer already onboarded with a participating bank. The document specifies the processes to be piloted, the attestations involved, and the partners participating in the cross-border pilot.

This is the v1.0 specification, consolidating the v0.7 review comments received on 12 May 2026 (Ard van der Heijden, ICTU) and the outcome of the PA1 review meeting held on 19 May 2026. The document targets v1.0 by 13 June 2026.

1.2 Scenario introduction

Scenario 5 demonstrates how the EUDI Wallet can be used to update specific customer information held by the bank after the initial onboarding. The MVP focuses on a single, well-bounded operation: updating the customer's Place of Residence. The user authenticates to the bank's online channel via session-level SCA (mechanism per Scenario 4 outcome), then presents an updated Place of Residence attestation. The bank verifies the attestation and updates its CRM and core banking systems. In the pilot, the relying party role is played by a mock bank application provided by OneSpan and by ABN AMRO as a real bank.

The scenario builds on the documentation already produced within the consortium, including:

- ARF version 2.8.x (the baseline for all pilots)
- The WP4 technical specification standards page for piloting.
- WE BUILD Stock Taking document PA1 v1.0
- Scenario 4 specification (session SCA mechanism)
- Scenarios 1A and 1B (initial onboarding) for upstream identity verification and customer establishment
- OpenID for Verifiable Presentations (OpenID4VP)
- OpenID for Verifiable Credential Issuance (OpenID4VCI)
- ETSI TS 119 472 (parts 1 and 3) for attribute attestation profiles
- Regulation (EU) 2024/1624 (AMLR); PSD2 Article 97; RTS Delegated Regulation 2018/389; PSR provisional agreement

Sequence diagrams and UX flow are maintained in the WP3 Technology and Standards GitHub area under PA1/Scenario 5.

2 Scenario specification

2.1 Introduction

Scenario 5 addresses a narrowly scoped but operationally important step of the CDD lifecycle: the update of a single customer attribute (Place of Residence) through the EUDI Wallet, without paper documentation and without branch visits. The wallet may carry the updated attribute (Place of Residence attestation) and, depending on the Scenario 4 outcome, the session SCA mechanism itself. The bank consumes the attestation, verifies it, and updates its records.

Two triggers are supported: customer-initiated (when the customer moves and proactively updates the data) and bank-initiated (when the bank's compliance system identifies the need for a periodic review or a remediation request).

2.1.1 Use Case and MVP Scope

MVP scope for Scenario 5 is limited to the update of Place of Residence. This narrows the v0.7 scope (which previously included Tax ID, Annual Income and Occupation) following the consortium decision of 19 May 2026 to maintain consistency across PA1 scenario documents and to keep the pilot focused on a well-bounded operation that can be concretely implemented and measured.

Rationale: Tax Identification Number is already contained in the PID and does not require a separate attestation update. Annual Income and Occupation are MVP+ for the pilot, as confirmed by Marie Austenaa's review comments. The Place of Residence update remains in MVP scope because it represents a typical CDD lifecycle event with material regulatory relevance (AMLR ongoing monitoring) and because it allows the consortium to exercise the full wallet-based update mechanics on at least one attribute.

The MVP is piloted as a single interoperability pilot. The relying party role is played by a mock bank application provided by OneSpan and by ABN AMRO as a real bank, the Izertis wallet is used for presentation, and the Place of Residence attestation is issued by qualified trust service providers in the participating countries: InfoCert for Italy and IDnow for Germany and Greece. Interoperability is exercised at the attestation level, across the national variations in address format and trust framework of IT, GR and DE, while the presentation and verification flow remains common. Possible national implications and follow-up actions may derive from the pilot outcome.

2.1.2 Wallet type

Scenario 5 uses the Natural Person Wallet only. Legal Person Wallets are not in scope for this scenario.

2.2 Scenario pre-conditions

2.2.1 Wallet and PID

The user has a valid, operational EUDI Wallet on their device, containing a non-expired PID issued by a trusted PID Provider. The PID is verifiable through the Trust infrastructure. Following the guidance from Ard van der Heijden, this is treated as a precondition rather than an in-scope step.

2.2.2 Prior customer relationship

The user has completed the bank onboarding (Scenario 1A or 1B). The bank holds the user's original KYC record, including the previous residence value, in its CRM and core banking systems. The account is active and in good standing.

2.2.3 Session-level SCA capability

The user is in a position to perform session-level Strong Customer Authentication when accessing the bank's online channel, in accordance with PSD2 Art. 97. The specific mechanism for this session SCA (the re-use of existing bank SCA methods, the use of an EUDI Wallet-based SCA attestation, or a combination) is being analysed within Scenario 4 of the PA1 use case. Scenario 5 is agnostic on the chosen mechanism and consumes whatever Scenario 4 finalises. For the duration of the pilot, the existing bank SCA method is assumed available as a fallback should Scenario 4 not be operational by start of testing. Critical dependency: if Scenario 4 has not finalised the session SCA mechanism by the start of pilot testing, Scenario 5 falls back on the existing bank SCA method already operational with the participating banks. Coordination with Scenario 4 leads is required to align the final architecture before pilot launch.

2.2.4 Place of Residence attestation issuance capability

For the pilot, the Place of Residence attestation is issued by a QTSP rather than by a municipal Authentic Source, since operational Authentic Sources for residence are not uniformly available across the pilot countries. The selected QTSPs are InfoCert for the Italian pilot and IDnow for the Greek and German pilots. The QTSP issues a synthetic Place of Residence QEAA after performing its own verification process. This is an explicit pilot workaround, not a position on the relative merits of QTSP versus Authentic Source issuance.

2.2.5 Technical infrastructure

For the pilot, the WE BUILD Trusted Lists serve as the operational source of trust anchors for the participating countries; operational national trust registries remain the target state. The bank's relying-party stack supports OpenID4VP. The bank's CRM and core banking systems support the address update integration.

2.2.6 Standardisation baseline

ARF version 2.8.x is the baseline. The Place of Residence attestation schema is to be aligned with the common semantic framework during the specification phase, using ISO 19160 and UPU S42 as references where applicable. The consortium credential scheme repository on GitHub is the reference for the Place of Residence attestation schema.

2.3 Main flow

The main flow describes the steps required to update the Place of Residence held in the bank's records through the EUDI Wallet. The flow is presented at the business level. Technical specifications by phase are in Section 3.

2.3.1 Steps 1-2: Trigger and notification

The bank's compliance system identifies the need to refresh the customer's residence data (periodic CDD review, expiring document, or change request received from the customer), or the customer proactively initiates the update via the banking portal or app. In the bank-initiated case, a notification is sent to the customer via the bank's standard communication channels.

2.3.2 Step 3: Access to the online banking

The customer navigates to the bank's online channel and selects the function to update the residence. The bank initiates a session-level SCA according to its established authentication policy (mechanism per Scenario 4 outcome).

2.3.3 Steps 4-5: Session SCA Authentication (MANDATORY)

The customer authenticates to the bank's online channel via Strong Customer Authentication, satisfying PSD2 Article 97. The mechanism used at this step (re-use of the

existing bank SCA, or use of an EUDI Wallet-based SCA attestation) follows the architecture being defined in Scenario 4 of the PA1 use case. For pilot purposes Scenario 5 is agnostic on the specific mechanism; the diagram in section 2.3.9 marks this step as MANDATORY to reflect the open coordination with Scenario 4.

2.3.4 Step 6: Bank requests Place of Residence attestation

Once authenticated, the bank issues an OpenID4VP Authorization Request for the updated Place of Residence attestation. The request specifies the attestation type, the required attributes via selective disclosure (street, number, postal code, city, country), the accepted trust level (QEAA from a QTSP listed in the trusted list), and a freshness requirement consistent with the bank's CDD policy. The Authorization Request is delivered to the wallet via QR code (cross-device flow) or deep link (same-device flow). Use of the Digital Credentials API is to be evaluated to optimise the user experience.

2.3.5 Steps 7-8: Attestation availability check; issuance if needed

The wallet receives the Authorization Request and checks whether a valid Place of Residence attestation is already present. Three sub-cases:

- Attestation present and valid: the wallet proceeds directly to Step 9.
- Attestation not present: the user initiates issuance from the designated QTSP. The QTSP authenticates the user via PID, performs its residence verification process, and issues a synthetic Place of Residence QEAA into the wallet via OpenID4VCI.
- Attestation present but expired or insufficient for the bank's freshness requirement: the user requests re-issuance from the QTSP as above.

2.3.6 Step 9: Presentation with consent

The wallet displays the Place of Residence attestation and the specific attributes that will be shared. The user reviews the values and authorises the presentation via wallet consent (biometric or PIN). The user's consent at this step authorises only the disclosure of the attestation; the explicit authorisation of the data change to be applied to the bank's records happens at Step 10 (see section 2.3.7) via a dedicated SCA. The wallet generates a verifiable presentation bound to the wallet instance, signs it, and transmits it to the bank via the OpenID4VP response endpoint.

The OpenID4VP consent at this step is a wallet-level consent on the disclosure of the attestation. It is distinct from the SCA at Step 10 (see Working Assumption 2.6.1), which authorises the specific data change being applied to the bank's records with transaction-specific binding.

2.3.7 Step 10: Authorise data change with SCA (MANDATORY)

Following the presentation, the bank initiates a dedicated SCA with transaction-specific binding to authorise the specific data change. The user sees the exact data values being applied to the bank's records (the new residence value extracted from the presented attestation) and authenticates explicitly to authorise that change. This Step 10 SCA is distinct from the session-level SCA at Steps 4-5: while the latter authenticates the user's identity for the session, the former authenticates the user's consent to the specific data change. The regulatory basis is PSD2 Article 97 (action through a remote channel implying risk of fraud or other abuses), RTS on SCA Article 26 (management and change of personalised security credentials), and PSR Article 85 (provisional political agreement). The PA1 partner meeting of 26 March 2026 confirmed SCA at Step 10 as the pilot default; the question is being escalated to the financial supervisory authorities (including Banca d'Italia) for authoritative interpretation.

2.3.8 Step 11: Verify attestation and update internal systems

After successful SCA at Step 10, the bank verifies the presented attestation: trust chain validation against the trust registry, revocation status check, signature verification using the issuer's qualified certificate, schema and attribute validation against the agreed Place of Residence schema, freshness assessment against the bank's CDD policy, and wallet binding verification with anti-replay challenge match. If all checks pass, the bank updates its CRM and core banking systems with the new residence value, records the wallet-based update in the audit trail (attestation issuer, issuance date, verification result, SCA evidence), and triggers any downstream compliance processes such as customer risk profile recalculation.

2.3.9 Step 12: Confirmation

The bank sends confirmation to the customer through the standard communication channel, including the updated residence value and the timestamp of the update. Optionally, a confirmation receipt may be delivered to the wallet.

2.3.10 Swimlane diagram

The swimlane below illustrates the Scenario 5 main flow consistent with the SCA architecture confirmed by the PA1 partner meeting of 26 March 2026 (see Working Assumption 2.6.1). Two SCA events are visible: one at Steps 4-5 for session-level authentication, and one at Step 10 with transaction-specific binding for data-change authorisation. The session-level SCA at Steps 4-5 is marked MANDATORY because the specific mechanism is being analysed in Scenario 4 of the PA1 use case; Scenario 5 will adopt whatever Scenario 4 finalises. The SCA at Step 10 is marked SCA REQUIRED with reference to PSD2 Art.97, RTS Art.26, PSR Art. 85.

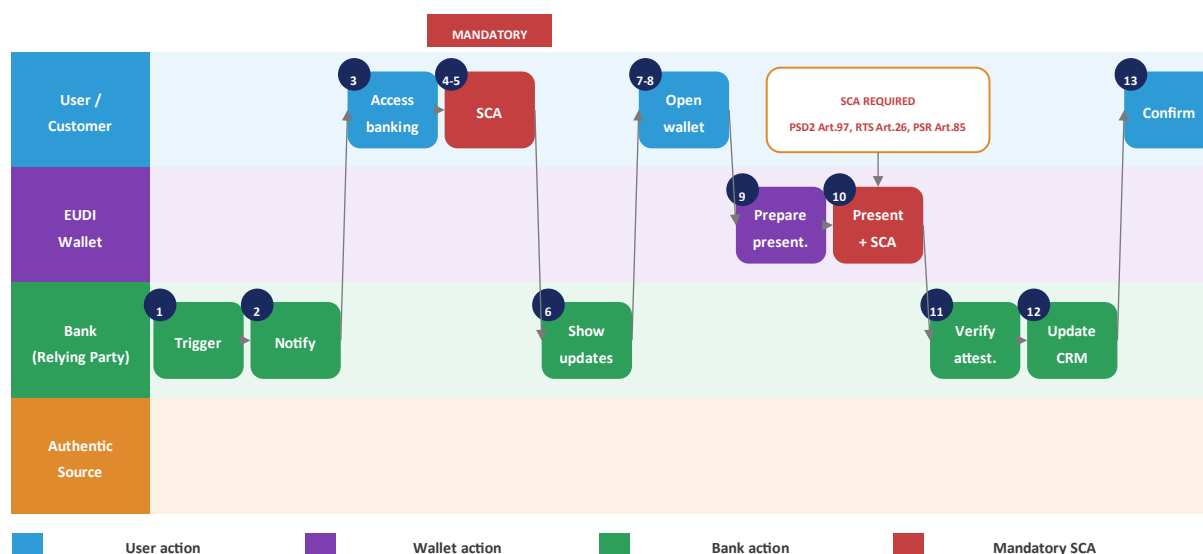


Figure 1 — Scenario 5 main flow swimlane, aligned with the SCA architecture confirmed on 26 March 2026

2.4 Scenario additional flows

Variations and exceptions piloted alongside the main flow are summarised below.

Variation / Exception	Description	MVP / MVP+
Same-device flow	User completes the whole process on a single device with the wallet installed.	MVP
Cross-device flow	User starts on desktop and completes authentication and	MVP

	presentation on a mobile wallet via QR code.	
Customer-initiated trigger	User proactively initiates the residence update after a move.	MVP
Bank-initiated trigger	Bank requests update during periodic CDD review or document remediation.	MVP
Attestation already present	Wallet holds a valid, non-expired Place of Residence attestation: skip issuance.	MVP
Re-issuance required	Attestation missing or expired: user requests issuance from the designated QTSP.	MVP
Use of intermediary	Bank may rely on an intermediary platform for the OpenID4VP exchange, mirroring Scenario 1B.	MVP+
Annual Income update	Future scope: update of income attestation. Out of MVP, retained as MVP+.	MVP+
Occupation update	Future scope: update of occupation attestation. Out of MVP, retained as MVP+.	MVP+
Expired wallet SCA attestation (if applicable)	If Scenario 4 produces an EUDI Wallet-based SCA attestation that expires, the user must re-obtain it via the Scenario 4 issuer before proceeding.	MVP (exception)
Trust chain failure	Verification fails at the bank: update is rejected and the customer is notified.	MVP (exception)
User cancels	User cancels at any point: no update is applied; bank records remain unchanged.	MVP (exception)

2.5 Challenges and barriers

The challenges below are those that remain after the scope reduction agreed on 19 May 2026. Several v0.7 challenges (notably the regulatory vs UX tension on a dedicated SCA at Step 10 and the complexity of multi-attestation updates) have been resolved or significantly reduced by the new scope and SCA architecture.

2.5.1 Absence of operational Authentic Sources for residence

Across the participating countries (IT, GR, DE), municipal population registries are not uniformly available as operational issuers of EUDI Wallet attestations for residence within the pilot timeframe. This is the main reason for relying on a QTSP-issued synthetic QEAA in the MVP. The mitigation is documented in Section 2.6.

2.5.2 Consistency with the PA3 banking position on root of trust

ABI Lab's position in PA3 emphasises a preference for identity verification anchored to Member State authentic sources (PID) rather than to QTSPs, on the basis of AMLR Art. 22(1) and the liability gap between the eIDAS and AMLR regimes. The reliance on a QTSP-issued residence attestation in Scenario 5 might appear inconsistent with that position. The two

cases are however qualitatively different: PA3 concerns identity verification at onboarding (CDD ex AMLR Art. 22), while Scenario 5 concerns the update of a single attribute for a customer already identified and verified via PID at the onboarding stage. The CDD ex Art. 22 has already been performed by the bank at account opening. The residence update is an ongoing-monitoring activity for which a QTSP-issued QEAA, used under the direct responsibility of the bank as the obliged entity, is acceptable. The mitigation is to document this distinction explicitly in the pilot and to flag that the long-term target remains Authentic Source issuance once available.

2.5.3 Attestation freshness and bank CDD policy

The intrinsic validity of a QTSP-issued residence attestation (12 months by default) may differ from a bank's CDD freshness policy in specific contexts. The bank can specify the freshness requirement as part of the OpenID4VP Authorization Request; the wallet handles the case of a still-valid but insufficiently fresh attestation by initiating a new issuance from the QTSP, rather than silently rejecting the attestation. This avoids confusing user experience.

2.5.4 Unstable and evolving standards

ARF 2.8.x is the baseline. OpenID4VP and OpenID4VCI are still evolving. The consortium fixates on the agreed baseline versions and accepts that interoperability testing may require alignment iterations during pilot.

2.5.5 Interoperability

The pilot exercises interoperability across IT, GR and DE. The Place of Residence attestation is issued by different QTSPs (InfoCert for IT, IDnow for DE and GR), exercising the national variations in address format and trust framework, while the presentation and verification flow through the Izertis wallet and the relying parties remains common. The schema for the Place of Residence attestation is designed with a common core to absorb these national differences.

2.5.6 Banking system integration

Updating a residence in core banking systems may require API or integration work. Where full automation is not feasible within the pilot, a semi-automated workflow with human validation is acceptable, clearly documented as a pilot limitation.

2.5.7 Dependency on Scenario 4

The session-level SCA mechanism at Steps 4-5 is being defined in Scenario 4. If Scenario 4 finalises an EUDI Wallet-based SCA attestation, Scenario 5 will consume it. If Scenario 4 is not operational by the start of pilot testing, Scenario 5 falls back on the existing bank SCA method already operational with the participating banks. Coordination with the Scenario 4 leads on architecture and timeline is required.

2.5.8 Trust infrastructure maturity

The trust registries, revocation services and trust anchor management must be operational across the pilot countries by the start of testing. Close coordination with the trust infrastructure is required; manual fallback verification is the contingency.

2.6 Working Assumptions

The following working assumptions establish the foundation on which Scenario 5 v1.0 is built. They reflect the 19 May 2026 meeting outcome and the v0.7 review feedback.

2.6.1 SCA architecture and data-change authorisation

The Scenario 5 main flow envisages two SCA events on the basis of the position consolidated by the PA1 partner meeting of 26 March 2026. Session-level SCA at Steps 4-5 authenticates

the user when accessing the bank's online channel, satisfying PSD2 Article 97. The specific mechanism for this session SCA (re-use of existing bank SCA methods, an EUDI Wallet-based SCA attestation, or a combination) is being analysed within Scenario 4 of the PA1 use case and is outside the scope of this document. Scenario 5 will adopt whatever Scenario 4 finalises. A dedicated SCA at Step 10 authorises the specific data change being applied to the bank's records, with transaction-specific binding to the value being modified (the new Place of Residence extracted from the presented attestation). The user sees the exact data and authenticates explicitly to authorise that change.

The normative basis for SCA at Step 10 is PSD2 Article 97 (any action through a remote channel implying risk of fraud or other abuses), RTS on SCA Article 26 (management and change of personalised security credentials, Delegated Regulation 2018/389), and PSR Article 85 (provisional political agreement of November 2025, which makes the requirement explicit for data change authorisation). The dedicated challenge is bound to the specific values being applied (transaction-specific binding terminology, used in this document to distinguish it from PSD2 "dynamic linking" which is reserved for payment authentication). The question is being formally escalated to the relevant financial supervisory authorities (including Banca d'Italia) for authoritative interpretation, in parallel with the pilot. The PA1 partner meeting of 26 March 2026 confirmed this assumption as the pilot default. The UX implementation of the SCA challenge (DC API vs deep link/app-switch) will be evaluated.

2.6.2 Validity period of the Place of Residence attestation

Default intrinsic validity for the pilot is 12 months, consistent with typical CDD update cycles. The bank may specify a tighter freshness requirement in the OpenID4VP request when supported by a regulatory basis (e.g. credit assessment under EBA/GL/2020/06, TUB Art. 120-undecies). The wallet handles the case of valid-but-insufficiently-fresh attestations by initiating new issuance from the QTSP rather than silently rejecting.

2.6.3 QTSP-issued synthetic attestation as pilot workaround

Place of Residence attestations are issued by a QTSP for the pilot, in absence of operational municipal Authentic Sources across the participating countries. The selected QTSPs are InfoCert for IT and IDnow for DE/GR. The QTSP verifies the residence prior to issuance using its standard processes (combination of utility bill, PID-bound residence claim, and any additional evidence required by its certificate practice statement). The attestation is a QEAA under eIDAS, signed with a qualified certificate, and registered in the trust list.

This is explicitly an MVP workaround. The long-term target remains Authentic Source issuance once municipal population registries are operational as EUDI Wallet attestation issuers. The pilot will produce a lesson-learned report documenting the operational, regulatory and user-experience implications of QTSP-based vs Authentic Source-based residence attestations.

2.6.4 Versions and protocols

ARF 2.8.x is the baseline. OpenID4VP and OpenID4VCI are used at the agreed baseline versions. SD-JWT VC is the credential format for the Place of Residence attestation (mdoc may be added as a secondary format if the common semantic framework so confirms).

2.6.5 Selective disclosure

Wallets in the pilot support selective disclosure. The bank requests only the attributes needed for the residence update (street, number, postal code, city, country) and not the entire attestation. Data minimisation under GDPR is the design principle.

2.6.6 Trust registry and revocation

The trust infrastructure provides operational trust registries with valid trust anchors for the pilot countries by the start of testing. Revocation is supported either via revocation lists or via OCSP-style services. The bank performs revocation checks before accepting the attestation.

2.6.7 Same-device and cross-device

Both same-device (deep link) and cross-device (QR code) flows are supported. The Digital Credentials API is evaluated as a way to optimise the user experience on same-device, in line with Marie Austenaa's comment on the v0.7.

2.6.8 Role of the intermediary

Intermediary use is MVP+ for Scenario 5. The architectural decision to standardise only the intermediary-to-wallet and intermediary-to-trust-framework interfaces (and to leave the intermediary-to-bank interface implementation-specific) is consistent with the broader PA1 alignment discussed in the 19 May meeting.

2.6.9 CRM and core banking update

Banks participating in the pilot have, or will develop during the specification phase, the capability to update the residence field in CRM and core banking systems automatically following successful attestation verification. Semi-automated workflows with human validation are acceptable as a pilot fallback.

2.6.10 Periodic review triggers

Bank-initiated triggers may be simplified to manual triggers by bank staff for the pilot. Production-grade automation of trigger detection is out of scope.

2.6.11 Natural Person Wallet only

Legal Person Wallets are out of scope for Scenario 5.

2.6.12 Partner commitment

All committed partners (banks, wallet providers, QTSPs) remain engaged through pilot completion. The list of committed partners is consolidated in Chapter 4 and reflects the current pilot composition, including OneSpan and ABN AMRO which joined in July 2026.

2.6.13 Review process

Working assumptions will be reviewed at v1.0 (13 June 2026), at the start of implementation, and at mid-pilot. The assumption on SCA architecture is the most sensitive to revision should supervisory guidance evolve.

3 Detailed scenario flow

This section provides implementation-level detail for each phase of the main flow. The reduced MVP scope makes the technical description considerably simpler than in v0.7.

3.1 Phase 1: Trigger and access

Customer-initiated: user opens the banking portal or app and selects "Update residence".

The banking system initiates the authentication request before any data request is sent.

Bank-initiated: the bank's compliance system identifies the customer due for residence update and sends a notification via the standard channel. The notification carries a deep link to the banking portal or app where the user starts the flow.

3.2 Phase 2: Session-level SCA Authentication

Protocol: OpenID4VP.

The bank performs session-level SCA at access to its online channel, satisfying PSD2 Article 97. The specific mechanism (re-use of existing bank SCA methods or use of an EUDI Wallet-based SCA attestation as defined in Scenario 4) follows the architecture being analysed in Scenario 4 of the PA1 use case. If an EUDI Wallet-based SCA attestation is adopted, the bank issues an OpenID4VP Authorization Request, the wallet authenticates the user via biometric or PIN and transmits the verifiable presentation, and the bank verifies trust chain, revocation, signature, account binding, and challenge match. If the existing bank SCA method is used, the bank applies its standard procedure. Scenario 5 is agnostic on the choice.

3.3 Phase 3: Bank requests Place of Residence attestation

Protocol: OpenID4VP.

The bank generates an OpenID4VP Authorization Request specifying:

- attestation type: Place of Residence
- required attributes via selective disclosure (street, number, postal code, city, country)
- accepted trust level: QEAA
- accepted issuers: trust list of registered QTSPs (InfoCert, IDnow, and any other QTSP issuing this attestation type)
- freshness requirement: maximum age of the attestation per bank CDD policy
- challenge/nonce; callback URL

3.4 Phase 4: Attestation availability check and issuance

The wallet evaluates the Authorization Request against the credentials it holds. If a valid Place of Residence QEAA satisfying schema and freshness is present, the flow proceeds to Phase 5. Otherwise, the wallet offers the user the option to obtain the attestation now or to cancel.

If the user proceeds, the wallet contacts the QTSP issuer via OpenID4VCI. The QTSP authenticates the user using the PID, performs its residence verification (compliant with its eIDAS certificate practice statement), issues the synthetic Place of Residence QEAA, signs it with a qualified certificate, and delivers it to the wallet. The wallet stores the attestation and returns to the Authorization Request flow.

3.5 Phase 5: Presentation with consent and submission

The wallet displays to the user the bank's identity (verified through the trust registry), the attestation that will be presented and the specific attributes that will be shared. The user reviews the values and authorises the disclosure of the attestation via biometric or PIN. The wallet generates the verifiable presentation, applies selective disclosure, signs the response with the wallet key, and transmits the response to the bank's callback URL. This consent

authorises the disclosure of the attestation only; the explicit authorisation of the data change to the bank's records is performed at the subsequent Step 10 SCA (see Phase 6 below).

The bank receives the response in the authenticated session that was established in Phase 2.

3.6 Phase 6: Step 10 SCA and verification

The bank initiates the dedicated SCA challenge at Step 10. The challenge is bound to the specific data values being applied to the bank's records (the new residence value extracted from the presented attestation); the user sees the exact change and authenticates explicitly. After successful SCA, the bank verifies the presented attestation in the following order:

- trust chain validation against the trust registry; confirmation that the issuer is on the QTSP trust list and authorised for this attestation type
- revocation status check (CRL or OCSP)
- signature verification using the issuer's qualified certificate
- schema and attribute validation against the agreed Place of Residence schema
- freshness assessment against the bank's CDD policy
- wallet binding verification (proof of possession) and challenge match (anti-replay)

If all checks pass, the verified residence value is taken as the authorised input for the CRM update.

3.7 Phase 7: Update of internal systems

The bank extracts the residence attributes from the verifiable presentation and maps them to the corresponding fields in CRM and core banking. The previous residence value is preserved in the audit trail alongside the new value, with the source recorded as wallet-based update via QEAA issued by the QTSP, received on the relevant timestamp, with session SCA evidence (mechanism used, issuer/validity if applicable). Downstream compliance triggers (if any) are fired.

3.8 Phase 8: Confirmation

The bank sends confirmation to the customer via the standard channel, including the updated residence value and the timestamp of the update. An optional confirmation receipt may be delivered to the wallet.

3.9 Summary table

Phase	Protocol / Technology	Key actions	Critical dependencies
1. Trigger and access	Bank portal/app	Notification or self-initiation; navigation to residence update	Bank UX
2. Authentication	OpenID4VP	Session-level SCA (mechanism per Scenario 4 outcome)	Scenario 4 (session SCA mechanism); existing bank SCA fallback
3. Request residence	OpenID4VP AR	Authorization Request with selective disclosure and freshness	Schema (common semantic framework)
4. Availability/Issuance	OpenID4VCI	Wallet checks; QTSP issuance if needed	QTSP (InfoCert/IDnow); PID
5. Presentation + consent	OpenID4VP	User review; wallet consent on disclosure; verifiable presentation transmitted	Wallet capability

6. SCA at Step 10 + verification	Trust chain + revocation	Dedicated SCA with transaction-specific binding; trust chain, revocation, signature, schema, freshness, wallet binding	trust registry
7. CRM/Core update	Bank integration API	Mapping; update; audit trail	Bank integration
8. Confirmation	Bank channels	Confirmation message; optional wallet receipt	Bank UX

Step-numbering note: the v1.0 phases above map onto the v0.7 14-step numbering with the following correspondence. Phase 2 (Steps 4-5) is session-level SCA, with mechanism deferred to Scenario 4. Phase 5 (Step 9) is wallet consent on the disclosure of the attestation. Phase 6 includes Step 10 (dedicated SCA with transaction-specific binding for the data change) and Step 11 (verification of the presented attestation). Phase 7 corresponds to Steps 12-13 (update of internal systems and audit trail).

4 Roles and participants

4.1 Scenario roles and committed partners

The following table lists the partners active in the scenario and the role each plays in piloting. Partner commitment is being consolidated for v1.0 per the 19 May meeting action item (scenario leads). The list reflects the state as of 19 May 2026 and is subject to final confirmation.

Primary role	Partner	Country	Role detail
User of EUDI Wallet	Test users in the participating countries	IT, GR, DE,	Natural persons piloting residence updates
Relying Party (Bank)	OneSpan	BE	Mock bank application, relying party of the pilot
Relying Party (Bank)	ABN AMRO	NL	Real bank relying party, alongside the OneSpan mock bank application
QTSP - Place of Residence issuer	InfoCert	IT	Issuer for IT; synthetic QEAA
QTSP - Place of Residence issuer	IDnow Trust Services	DE	Issuer for DE and GR; synthetic QEAA
Intermediary platform (MVP+)	TBC	TBC	Per 19 May meeting: intermediary role to be defined; MVP+ status

Action item open (Anzellotti, ABI Lab): coordination with the identified QTSPs to confirm scope, schema and timeline of the synthetic Place of Residence QEAA issuance, with priority on InfoCert for the IT pilot and IDnow for the DE/GR pilots.

4.2 Additional roles and ecosystem partners

Ecosystem partners providing wallet instances, PID issuance and trust infrastructure for Scenario 5 are listed below.

Primary role	Partner	Country	Role detail
EUDI Wallet Provider	Izertis	IT, GR, DE	Wallet used in the interoperability pilot
PID Provider	PID Provider group	IT, GR, DE	PID issuance per national eID schemes
Trusted List / Trust Registry	Trust Infrastructure	EU-wide	Trust registries and revocation services

4.3 Requirements

The functional, organisational and technical requirements for each role are in Annex 1. Requirements are scoped to the MVP focus (Place of Residence update). Generic requirements that apply to all scenarios (e.g. wallet provider must provide a wallet) are not duplicated here; the requirements listed are those specific to Scenario 5.

5 Attestations

5.1 Introduction

Scenario 5 produces and consumes the Place of Residence attestation (issued by a QTSP for the pilot). It also consumes the session SCA mechanism, whose specific design is being defined in Scenario 4 of the PA1 use case. It does not create new attestations within this scenario. The Place of Residence schema and rulebook are developed in coordination with the common semantic framework. Income and Occupation attestations remain MVP+ and are out of scope for this document.

5.2 Attestations consumed but produced by other scenarios or WGs

Attestation	Description	Provided by	For countries	Notes
PID	Personal Identification Data. Foundational credential used by the QTSP to authenticate the user at the moment of issuing the Place of Residence attestation.	PID Provider group	IT, GR, DE	Precondition. Issued per national eID schemes.
Session SCA mechanism	Mechanism used to perform session-level SCA at the bank's online channel at Steps 4-5. Specific design under analysis in Scenario 4 of the PA1 use case.	Scenario 4 (PA1)	IT, GR, DE	Mechanism deferred to Scenario 4. Scenario 5 fallback: existing bank SCA method.

5.2.1 Created attestations overview

The table below summarises the attestations referenced in Scenario 5 and their MVP status. The rulebook for the only attestation in MVP scope (Place of Residence) is detailed in section 5.3 below.

Attestation Name	Short Description	For Countries	Applicable Domain Standards	Status
Place of Residence	Current residential address of the user. Issued by the designated QTSP (InfoCert for IT; IDnow for DE/GR) as a synthetic QEAA, after verification per the QTSP's certificate practice statement.	IT, GR, DE	ISO 19160; UPU S42; ETSI TS 119 472	MVP — in scope
Tax Identification Number	Already conveyed by the PID; no separate update attestation required in this scenario.	—	—	Removed (covered by PID)
Annual Income	Annual gross or net income. Issuance and rulebook deferred.	—	EBA/GL/2020/06 (reference)	MVP+ (deferred)
Occupation	Current professional occupation or employment status. Issuance and rulebook deferred.	—	ISCO-08 (reference)	MVP+ (deferred)

Table — Attestations referenced in Scenario 5 (MVP and MVP+ status)

5.3 Place of Residence attestation

Place of Residence is the only attestation actively produced and consumed within Scenario 5 in the MVP scope. The attestation rulebook is developed jointly by ABI Lab and Banca Sella for the business requirements and by the common semantic framework for the technical schema. The attestation is a QEAA under eIDAS, issued by a QTSP, and signed with the QTSP's qualified certificate.

Field	Value
Attestation type	Place of Residence (QEAA)
Issuer (pilot)	InfoCert (IT); IDnow (DE/GR)
Trust level	QEAA (highest)
Format	SD-JWT VC (primary); mdoc (secondary, if confirmed by the common semantic framework)
Mandatory attributes	street, number, postal code, city, country, issuance_date, expiry_date, issuer_id
Optional attributes	country-specific extensions (e.g. comune for IT; Bundesland for DE) as defined by the common semantic framework
Default validity	12 months
Selective disclosure	Required (SD-JWT VC)
Reference standards	ISO 19160 (address); UPU S42 (postal address); ETSI TS 119 472 (attribute attestation profile)
Status	Fit-for-pilot schema; rulebook in development with the common semantic framework

Issuance prerequisites for the QTSP: the QTSP authenticates the user via PID, verifies the residence claim using its certificate practice statement procedures, issues the QEAA, and delivers it to the wallet via OpenID4VCI. The verification record is retained by the QTSP for audit purposes.

Alignment notes:

- Coordination on the common address schema is the action with the highest dependency risk for v1.0 delivery.
- Coordination with BU2 (cross-use of address-like attributes in business contexts) is recommended but not blocking.
- Future production target: replace the QTSP-issued synthetic QEAA with an Authentic Source-issued attestation from municipal population registries, once available.

6 Annex 1 - Requirements for scenario roles

Requirements are listed by role with the MoSCoW priority: MUST, SHOULD, COULD, WON'T. Type: F (functional), O (organisational), T (technical). Only requirements specific to the residence-update flow are listed; generic requirements that apply universally to wallet providers, banks or trust services are not duplicated.

6.1 User of EUDI Wallet

ID	Requirement	Type	Priority
U-F1	Must hold a valid PID and have the means to perform session-level SCA at the bank's online channel before initiating the residence update. The specific SCA mechanism follows the outcome of Scenario 4.	F	MUST
U-F2	Must authenticate to the bank's online channel via session-level SCA (mechanism per Scenario 4 outcome).	F	MUST
U-F3	Must be able to request a Place of Residence QEAA from the designated QTSP via OpenID4VCI if not already present in the wallet or if the existing one does not meet the bank's freshness requirement.	F	MUST
U-F4	Must review the residence value in the wallet before consenting to the presentation.	F	MUST
U-F5	Must authorise the presentation via biometric or PIN.	F	MUST
U-T1	Device capable of running the wallet application and supporting biometric or PIN authentication.	T	MUST
U-T2	Stable internet connection.	T	MUST

6.2 Relying Party (Bank)

ID	Requirement	Type	Priority
----	-------------	------	----------

B-F1	Must be able to trigger the residence update (periodic CDD review, document remediation, or customer-initiated).	F	MUST
B-F2	Must perform session-level SCA at access to the online channel, per the mechanism finalised in Scenario 4 of the PA1 use case.	F	MUST
B-F3	Must request the Place of Residence attestation via OpenID4VP, specifying selective disclosure and freshness.	F	MUST
B-F3b	Must apply a dedicated SCA with transaction-specific binding at Step 10, before applying the data change to the bank's records (PSD2 Art. 97, RTS Art. 26, PSR Art. 85).	F	MUST
B-F4	Must verify the presented attestation: trust chain, revocation, signature, schema, freshness, wallet binding, anti-replay.	F	MUST
B-F5	Must update the residence field in CRM and core banking systems with audit trail of the attestation issuer, validity and verification result.	F	MUST
B-F6	Must send confirmation to the customer through the standard channel.	F	MUST
B-F7	Should document and apply use-case-specific freshness requirements beyond the default 12 months only where supported by a regulatory basis.	F	SHOULD
B-O1	Must integrate the wallet-based residence update into existing CDD remediation workflows.	O	MUST
B-O2	Must maintain a fallback for cases where verification fails (manual handling, customer outreach).	O	MUST
B-T1	Must implement OpenID4VP for Place of Residence requests; the OpenID4VP usage for session SCA depends on the Scenario 4 outcome.	T	MUST
B-T2	Must integrate with trust registry and revocation services.	T	MUST
B-T3	Must support QR code (cross-device) and deep link (same-device) delivery.	T	MUST
B-T4	Should evaluate use of the Digital Credentials API to improve same-device user experience.	T	SHOULD

6.3 QTSP (Place of Residence issuer)

ID	Requirement	Type	Priority
QT-F1	Must issue Place of Residence QEAA upon request from the user wallet via OpenID4VCI.	F	MUST
QT-F2	Must authenticate the user via PID before issuance.	F	MUST

QT-F3	Must verify the residence claim using the procedure declared in its certificate practice statement.	F	MUST
QT-F4	Must sign the QEAA with a qualified certificate.	F	MUST
QT-F5	Must publish issuer metadata and certificates to the trust registry.	F	MUST
QT-F6	Must maintain revocation status and provide a revocation interface (CRL or OCSP).	F	MUST
QT-F7	Must retain the verification record for audit purposes per its CPS.	F	MUST
QT-O1	Must be a qualified TSP under eIDAS.	O	MUST
QT-O2	Must coordinate with the common semantic framework on the attestation schema.	O	MUST
QT-T1	Must implement OpenID4VCI.	T	MUST
QT-T2	Must support SD-JWT VC as the primary credential format (mdoc as secondary if confirmed by the common semantic framework).	T	MUST

6.4 EUDI Wallet Provider

ID	Requirement	Type	Priority
WP-F1	Must support OpenID4VP for Place of Residence presentation. Support for OpenID4VP-based session SCA presentation depends on the Scenario 4 outcome.	F	MUST
WP-F2	Must support OpenID4VCI for receiving the Place of Residence QEAA from the QTSP.	F	MUST
WP-F3	Must implement selective disclosure (SD-JWT VC).	F	MUST

WP-F4	Must display the residence value being shared and require user consent (biometric or PIN) before transmission.	F	MUST
WP-F5	Must handle the case of an absent or insufficient attestation by offering re-issuance from the QTSP.	F	MUST
WP-F6	Must support both same-device (deep link) and cross-device (QR) flows.	F	MUST
WP-F7	Should evaluate Digital Credentials API for same-device UX optimisation.	F	SHOULD

6.5 Key dependencies

The dependencies below are critical for pilot success:

- Scenario 4 session SCA mechanism: finalisation needed before pilot launch. Fallback: existing bank SCA method.
- the common semantic framework: schema for Place of Residence aligned and confirmed.
- Trust infrastructure: trust registries and revocation services operational for the pilot countries.
- QTSP coordination: InfoCert (IT), IDnow (DE/GR) confirmed.
- Wallet providers: Izertis, capable of OpenID4VP and OpenID4VCI for the Place of Residence flow.

7 Annex 2 - Glossary

Term / Acronym	Definition
AMLR	Anti-Money Laundering Regulation (EU) 2024/1624.
ARF	Architecture Reference Framework for the EUDI Wallet ecosystem. Pilot baseline: v2.8.x.
Authentic Source	Authoritative entity that holds and can attest to specific data about a person. In this scenario the production target for Place of Residence; replaced for the pilot by a QTSP-issued QEAA.
CDD	Customer Due Diligence under AML legislation.
CRM	Bank's Customer Relationship Management system.
DC API	Digital Credentials API. Browser/OS-level API for presentation flows; under evaluation.
EAA	Electronic Attestation of Attributes.
eIDAS / eIDAS 2.0	Regulation (EU) 910/2014 as amended, establishing the legal framework for electronic identification and trust services and the EUDI Wallet.
EUDIW	European Digital Identity Wallet.
KYC	Know Your Customer.
MVP	Minimum Viable Product. In Scenario 5 v1.0: Place of Residence update only.
OpenID4VCI	OpenID for Verifiable Credential Issuance. Protocol used by the QTSP to issue the Place of Residence QEAA to the wallet.
OpenID4VP	OpenID for Verifiable Presentations. Protocol used by the bank to request the Place of Residence attestation from the wallet, and (subject to Scenario 4 outcome) the session SCA attestation.
PID	Personal Identification Data. Foundational credential in the wallet.
PSD2	Payment Services Directive 2 (EU) 2015/2366.
PSR	Payment Services Regulation (provisional political agreement, November 2025).
QEAA	Qualified Electronic Attestation of Attributes.
QTSP	Qualified Trust Service Provider under eIDAS. Pilot issuers for Place of Residence: InfoCert (IT); IDnow (DE/GR).
RTS	Regulatory Technical Standards on SCA (Delegated Regulation 2018/389).
SCA	Strong Customer Authentication.
SCA attestation (wallet-based)	Candidate authentication attestation under definition in Scenario 4. Scenario 5 will adopt it if and when Scenario 4 finalises it; otherwise the existing bank SCA method is used at Steps 4-5.
SD-JWT VC	Selective Disclosure JWT Verifiable Credential. Primary credential format for the Place of Residence attestation in the pilot.

Scenario 1A/1B	PA1 scenarios for cross-border personal account opening. Precondition for Scenario 5.
Scenario 4	PA1 scenario analysing the issuance of banking attestations to the wallet (including a possible SCA attestation, SCA-IBAN, IBAN Ownership). The session SCA mechanism for Scenario 5 will follow the Scenario 4 outcome.
TUB	Testo Unico Bancario. Italian consolidated banking law.
Transaction-specific binding	The cryptographic linkage of the user's strong authorisation to the specific values being modified, applied at the dedicated Step 10 SCA in Scenario 5. The user sees the exact data being applied to the bank's records and authenticates explicitly to authorise that change. The terminology distinguishes this binding from PSD2 "dynamic linking", which is reserved for the payment authentication context.
WE BUILD	EU-funded Large-Scale Pilot (Grant Agreement 101224751).
WP3	Work Package 3: Wallet for Payment and Banking.

WE BUILD consortium

Specification Scenario A.1 – A2A SCA

WP3 – PA2 Consumer payments

Date : 2026-06-20
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
2.1.1	High level flows from the Stock Taking phase	6
2.1.2	Detailed Flows	7
2.2	<i>Scenario flows.....</i>	8
2.2.1	Flow 1: Issuer-requested A2A SCA flow	8
2.3	<i>Challenges and barriers.....</i>	16
2.3.1	Wallet invocation mechanism maturity (DC API vs deep-link)	16
2.4	<i>Working Assumptions.....</i>	16
2.4.1	Issuer-requested SCA model.....	16
2.4.2	Scope limited to payment authentication only	16
2.4.3	No combined presentation in issuer-requested flows.....	16
2.4.4	Attestation issuance as a pre-condition	16
2.4.5	Optional wallet invocation mechanisms	16
2.4.6	Trust infrastructure availability	17
2.4.7	Bank policy variability	17
3	Roles and participants.....	17
3.1	<i>Roles represented in the scenario</i>	17
3.2	<i>Scenario roles and participants</i>	18
3.3	<i>Additional roles and partners</i>	18
3.4	<i>Target country combinations</i>	19
3.5	<i>Requirements.....</i>	19
4	Attestations.....	20
4.1	<i>Introduction.....</i>	20
4.2	<i>Attestations to be provided by other UCs/WGs/scenarios</i>	20
4.3	<i>Created attestations in the scenario.....</i>	21
	Annex 1 – Requirements for scenario roles	22
	Annex 2 – Sequence Diagrams	23

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario A1 A2A SCA, as part of use case PA2 in work package 3 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.

A separate MVP+ specification document expands the scope with additional features and requirements.

1.2 Scenario introduction

This scenario pilots cross-border Strong Customer Authentication (SCA) for Account-to-Account (A2A) “Pay-by-Bank” payments, using the EU Digital Identity Wallet (EUDIW) as an alternative bank-led authentication method in Open Banking payment flows.

It is part of a wider set of scenarios that have been developed in PA2:

- A1 Account-based online payment SCA with the EUDIW
- A2 Account-based payment initiation with the EUDIW
- B1 Card-based online payment SCA with the EUDIW
- B2 Card-based payment initiation with the EUDIW

Technology / Specification	Publication URL
ARF v2.9	https://eudi.dev/2.9.0/architecture-and-reference-framework-main/#1-introduction
ARF Technical Specification 12 v1.0.1	https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts12-electronic-payments-SCA-implementation-with-wallet.md
EMVco Digital Payment Credential Draft 1.0 (19th Jan 2026)	WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=7934&fid%5B0%5D=201&fid%5B1%5D=215&fid%5B2%5D=1232
W3C Digital Credentials API	https://www.w3.org/TR/digital-credentials/
PSD2 (Directive (EU) 2015/2366)	https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng

eIDA2 Regulation on SCA (Recital 62 and Article 5f2)	https://eur-lex.europa.eu/eli/reg/2024/1183/oj
WE BUILD WP3 PA2 Stock Taking 1.01	WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=5920&fid%5B0%5D=201&fid%5B1%5D=202&fid%5B2%5D=4208
EWG Implementation Guide 1.2	WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=866&fid%5B0%5D=201&fid%5B1%5D=202
SD-JWT VC (IETF draft)	https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/
OID4VCI 1.0	https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
OID4VP 1.0	https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
W3C Verifiable Credentials Data Model	https://www.w3.org/TR/vc-data-model/

2 Scenario specification

2.1 Introduction

This scenario covers the use of the EU Digital Identity Wallet (EUDIW) as an alternative Strong Customer Authentication (SCA) method for Account to Account (A2A) Pay by Bank payments initiated via Open Banking. It focuses on issuer-requested (aka “bank-led”) authentication, where the bank uses the EUDIW to authenticate its customer during payment authorisation, instead of relying on proprietary SCA mechanisms such as bank mobile applications.

In Scenario A1, the bank remains the sole relying party for authentication throughout the flow. Merchants and Payment Initiation Service Providers (PISPs) do not request credentials from the wallet and have no direct interaction with the EUDIW during the SCA step. The scenario also aims to demonstrate cross-border interoperability, whereby an SCA attestation issued by a bank in one Member State can be used to authenticate an A2A payment to a merchant located in another Member State, within the WE BUILD trust framework.

Attestation issuance for the pilot was guaranteed by participating banks, which also take part in PA1 Scenario 4 and will issue SCA-IBAN attestations to their customers during pilot onboarding.

Scenario A1 is part of Use Case PA2 (Consumer Payments) under Work Package 3 of the WE BUILD consortium and is included in the MVP scope. The scenario uses a Natural Person EU Digital Identity Wallet; Legal Person Wallets are out of scope.

Overview and key characteristics:

- Authentication model: Issuer-requested; the bank authenticates the consumer using the EUDIW during payment authorisation.
- Relying party model: The bank is the only relying party; merchants and PISPs do not access or receive wallet credentials.
- Cross-border scope: Supports authentication of payments where the consumer, bank and EU Digital Identity Wallet are located in the same Member State, while the merchant is located in a different Member State.
- Wallet invocation: The EUDIW may be invoked using W3C Digital Credential APIs (DC API) where supported, or via deep-link / native mechanisms as a fallback. These are treated as implementation variants of the same functional flow.
- Supported attestations:
 - SCA-IBAN (payment instrument bound) and
 - SCA-User (user level).
- In line with TS12 payment confirmation principles, Scenario A1 treats payment-instrument-bound attestations (SCA-IBAN) as the default model for issuer-led A2A SCA.

- Support for user-level attestations (SCA-User) is included as a deliberate pilot extension (see MVP+ document) to evaluate feasibility and user experience in cases where instrument-bound credentials are not available.

2.1.1 High level flows from the Stock Taking phase

The stock taking phase has confirmed the following scope for the A1 pilot scenario:

ID	Scenario name	Description	Attestations to use	Proximity or Remote	MVP
A1	A2A on-line SCA	Issuance of SCA attestation from bank portal (idem B1) – use of EU-DIW for Open Banking online payment SCA – bank-led SCA - Connection to WE BUILD Trust infrastructure	- SCA IBAN	Remote	Y
A1 +	Advanced A2A on-line SCA	A1 + one or many of: SCA attestation lifecycle management; PISP-captured SCA; Merchant captured SCA; combined presentation (age verification as a priority) with DC APIs;	- SCA Attestation - PID for age Depending on partners, other attestations may be used (eg Student, Loyalty, eReceipt, ...)	Remote	N

During the specification phase, the scope of Scenario A1 has been intentionally refined compared to the initial Stock Taking definition in order to ensure a clear separation of responsibilities between scenarios and to maintain a feasible and focused MVP.

Clarification on attestation issuance and verification

During the specification phase, it was clarified that Scenario A1 cannot rely on attestation issuance performed solely in PA1. For the purposes of the PA2 pilot, an SCA-IBAN attestation must be issued by a bank that also participates in PA1 and acts as the relying party during payment authentication.

While WP3 T&S group remains responsible for defining the specification and standards for SCA-IBAN attestation issuance, issuance and verification for Scenario A1 must be performed by the same PA2 bank.

Combined presentation (i.e. payment authentication combined with the disclosure of additional attributes such as age or other identity attestations) has been excluded from Scenario A1. This decision was taken because in issuer-requested Open Banking flows, the bank remains the relying party for authentication and there is no direct interaction between the merchant and the wallet during the SCA step.

Supporting combined presentation in this context would introduce additional technical and organisational complexity without being representative of current Open Banking payment patterns. Combined presentation is therefore addressed in scenarios where the merchant or a third party actively requests credentials.

Merchant-captured or PISP-captured SCA flows have also been excluded from Scenario A1. These flows require the merchant or PISP to act as the relying party requesting credentials from the wallet and are covered under **Scenario A2 (A2A Payment Initiation)**.

As a result of these decisions, Scenario A1 is limited to issuer-requested (bank-led) SCA flows and does not include any additional attestations beyond those strictly required for payment authentication.

The MVP for Scenario A1 consists of issuer-requested A2A SCA using:

- SCA-IBAN attestation,
- same-device journey,
- invocation via DC API or deep-link if DC API is not possible on a device.

All other variants (SCA-User, cross-device journeys) are considered extensions and are documented separately in MVP+ document.

ID	Scenario name	Description	Attestations to use	Proximity or Remote	MV P
A1	A2A on-line SCA	Issuer-requested Strong Customer Authentication for Open Banking “Pay-by-Bank” payments, where the bank uses the EU Digital Identity Wallet (EUDIW) to authenticate the user during payment authorisation. For the purposes of the PA2 pilot, issuance of the SCA attestation is in scope and is performed by the participating bank, in accordance with PA1 specifications.	- SCA-IBAN	Remote	Y

2.1.2 Detailed Flows

The partners have agreed on the following relevant flows, and selected a few to be part of the MVP

ID	Flow name	Description	Attestations to use	Proximity or Remote	MV P
A1-F1	Issuer-requested A2A SCA	Issuer-led Open Banking A2A payment flow where the bank invokes the EU Digital Identity Wallet (EUDIW) to authenticate the consumer during payment authorisation.	SCA-IBAN	Remote	Y

		The flow supports SCA-IBAN attestation bound to a specific payment account. The wallet is invoked using DC API or deep-link on the same device.			
--	--	---	--	--	--

2.1.2.1 Out-of-scope flows

The following flow types are explicitly out of scope for Scenario A1 and are therefore not described further in this document:

- Merchant-captured or PISP-captured SCA flows, where the merchant or a third party acts as the relying party (covered under Scenario A2).
- Combined presentation flows, where payment authentication is combined with the disclosure of additional attributes (e.g. age or other identity claims).
- Payment initiation flows where the wallet directly signs or initiates the payment.

2.2 Scenario flows

2.2.1 Flow 1: Issuer-requested A2A SCA flow

2.2.1.1 Main flow description

1. User story:

As a consumer paying at an online merchant using an Open Banking “Pay-by-Bank” payment method, I want my bank to authenticate me using my EU Digital Identity Wallet (EUDIW), so that I can securely authorise the payment using a standard, cross-border Strong Customer Authentication mechanism instead of my bank’s proprietary authentication method.

2. Description

In this issuer-requested flow, the user initiates a payment at an online merchant and selects an Open Banking “Pay-by-Bank” option. The consumer is redirected to their bank, either directly or via a Payment Initiation Service Provider (PISP) to authorise the payment.

During the payment authorisation step, the bank invokes the consumer’s EUDIW to perform Strong Customer Authentication. After authentication (wallet unlock), the wallet presents the SCA attestation, previously issued by the bank and prompts the consumer to authenticate and consent to its use for the specific payment transaction.

Upon successful authentication, the EUDIW presents the attestation to the bank. The bank verifies the attestation, completes the SCA step and proceeds with the payment authorisation according to existing Open Banking and SEPA payment flows. The merchant and any involved PISP are only informed of the payment outcome.

2.2.1.2 Additional flows

The issuer-requested A2A SCA flow described above may be realised using wallet invocation mechanisms and user journeys, depending on device capabilities, operating system support, and bank implementation choices. These variants do not change the functional scope of Scenario A1 and are considered alternative implementations of the same issuer-requested flow.

The bank may invoke the consumer's EUDIW using different technical mechanisms, depending on platform support:

- **Invocation via W3C Digital Credential APIs (DC API)**, where supported by the user agent, operating system, and wallet provider.
- **Invocation via deep-link or equivalent native mechanisms**, used as an alternative where DC API support is not available or not enabled.

The choice of invocation mechanism does not affect the roles, responsibilities, or trust relationships defined for Scenario A1. However, as can be seen in UX flows, choice of the invocation mechanisms impact user experience.

In all cases, the bank remains the relying party for authentication and receives the SCA attestation directly from the wallet.

The table below summarises all variants possible in the MVP.

Variant	Attestation used	Device	Invocation mechanism	MVP
V1	SCA-IBAN	Same-device	DC-API	Yes
V2	SCA-IBAN	Same-device	Deep-link	Yes

The following non-happy path may occur across all issuer-requested A2A SCA flows described in Scenario A1. These cases do not introduce additional functional flows, but result in termination or fallback within the existing Open Banking payment journey.

- **Wallet not available or invocation fails**
If the EU Digital Identity Wallet (EUDIW) cannot be invoked (e.g. not installed, technical error), the payment authorisation cannot proceed using wallet-based SCA. The bank may fall back to an existing proprietary SCA method or abort the payment.
- **Consumer cancels wallet interaction**
If the user aborts or declines the wallet authentication or attestation presentation, the SCA step is not completed and the payment authorisation fails. The consumer is returned to the payment context and may select an alternative payment method.
- **SCA attestation not present, expired or revoked**
If the required SCA-IBAN attestation is not available in the wallet, or is no longer valid, the bank

cannot complete SCA using the EUDIW. The payment fails and the consumer may be prompted to complete attestation issuance outside of the payment flow.

- **Attestation verification fails**
If the bank cannot verify the presented attestation (e.g. invalid signature, untrusted issuer), the SCA step fails and the payment is not authorised.
- **Payment declined after successful SCA**
Even after successful wallet-based SCA, the bank may decline the payment for other reasons (e.g. insufficient funds, fraud detection). In such cases, the merchant and any involved PISP are informed of the payment outcome according to existing Open Banking flows.

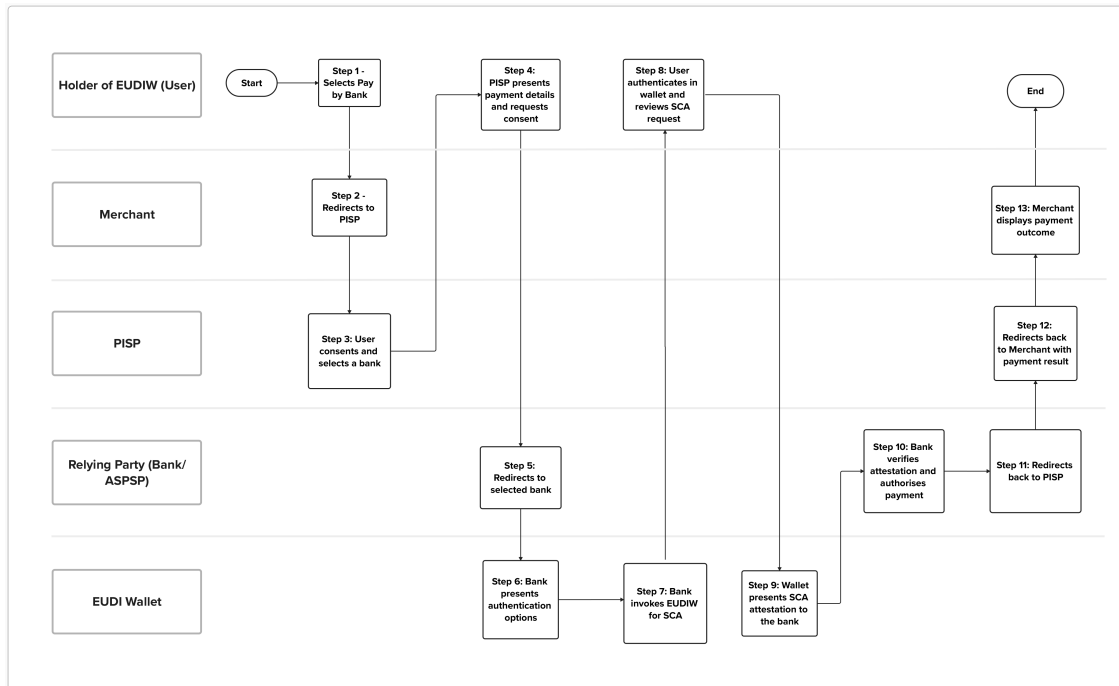
2.2.1.3 *Pre-conditions*

The following pre-conditions apply to the issuer-requested A2A SCA flow:

- The consumer has an active **Natural Person EU Digital Identity Wallet (EUDIW)** installed and operational on at least one device.
- The consumer is an existing customer of the bank and has an eligible payment account that supports Open Banking A2A payments.
- An **SCA Attestation** has already been issued by the bank and is available in the consumer's EUDIW.
- The bank supports the use of the EUDIW as an alternative SCA method for Open Banking payment authorisation.
- An Open Banking A2A payment has been initiated at an online merchant using a "Pay-by-Bank" payment option, either directly or via a Payment Initiation Service Provider (PISP).
- The trust infrastructure required to verify the SCA attestation (e.g. issuer trust lists and cryptographic verification material) is in place.

The issuance, lifecycle management (e.g. renewal, suspension, revocation) of the SCA attestation into the EUDIW are considered **out of scope** for this flow and are addressed elsewhere in the PA1 specification set.

2.2.1.4 Flow steps



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
Step 1: User selects “Pay by Bank” at merchant checkout	Consumer / Merchant	Consumer initiates checkout at the merchant and selects an Open Banking “Pay-by-Bank” payment option.	Merchant supports Open Banking payments via a PISP.	-
Step 2: Redirect to PISP	Merchant → PISP	Merchant redirects the user to the Payment Initiation Service Provider (PISP) to initiate the Open Banking payment flow.	Merchant–PISP integration in place.	-
Step 3: Bank selection	Consumer / PISP	Consumer selects their bank (ASPSP) from the list of supported banks provided by the PISP.	-	Variation: Bank may already be pre-selected (e.g. selected on Merchant’s checkout, returning consumer).
Step 4: PISP presents payment details and requests consent	PISP / Consumer	PISP presents payment details (amount, payee, reference) and requests consumer’s consent to initiate the payment, as required under PSD2.	-	-

Step 5: Redirect to bank for payment authorisation	PISP → Bank	PISP redirects the consumer to the selected bank's authorisation endpoint to continue the Open Banking payment flow.	-	-
Step 6: Bank presents authentication options	Bank / Consumer	The bank presents the available Strong Customer Authentication options to the consumer in the payment authorisation context. This may include existing bank authentication methods as well as authentication using the EU Digital Identity Wallet (EUDIW).		-
Step 7: Bank invokes EU-DIW for SCA	Bank / Wallet / Consumer	When the consumer selects the EU Digital Identity Wallet as the authentication method, the bank invokes the wallet to perform Strong Customer Authentication of the payment.	Wallet available and invocation possible (see Invocation variants).	SCA-IBAN attestation is presented
Step 8: User authenticates in wallet and reviews SCA request	Wallet / Consumer	Wallet prompts user authentication (e.g. biometrics) and displays the SCA attestation to the consumer for confirmation in the context of the payment.	User has access to wallet authentication; attestation present.	-
Step 9: Wallet presents SCA attestation to the bank	Wallet → Bank	Wallet presents the SCA attestation to the bank as part of the SCA process.	-	-
Step 10: Bank verifies attestation and authorises payment	Bank	Bank verifies the attestation, completes the SCA step and authorises the payment.	-	-
Step 11: Redirect back to PISP	Bank → PISP	Consumer is redirected back to the PISP	-	-
Step 12: Redirect back to Merchant	PISP → Merchant	PISP presents payment confirmation and redirects back to Merchant		
Step 13: Merchant	Merchant / Holder	Merchant displays confirmation or failure of the	-	-

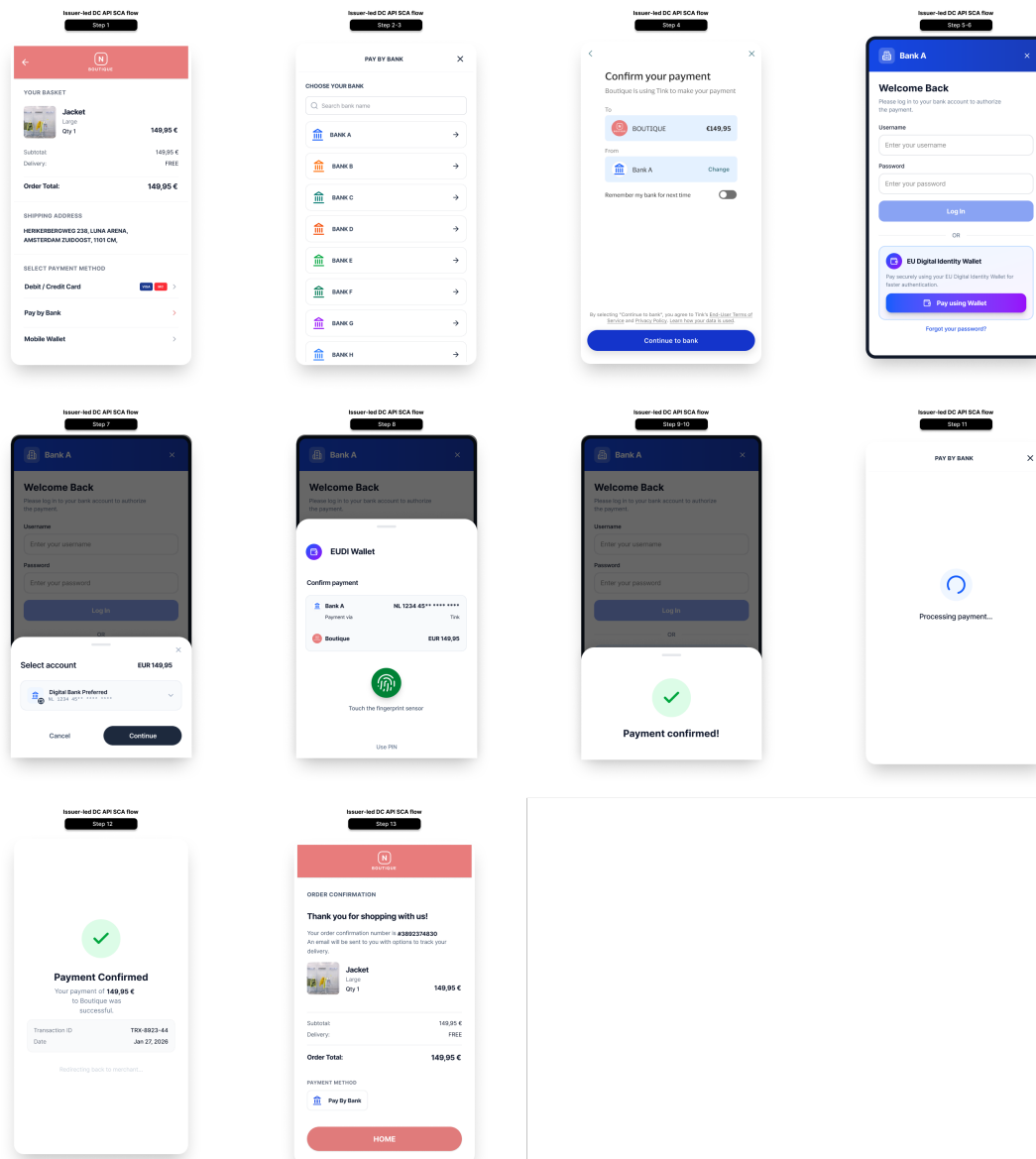
displays payment outcome		payment to the Consumer.		
---------------------------------	--	--------------------------	--	--

Depending on the variation described in the previous section, there are the following changes:

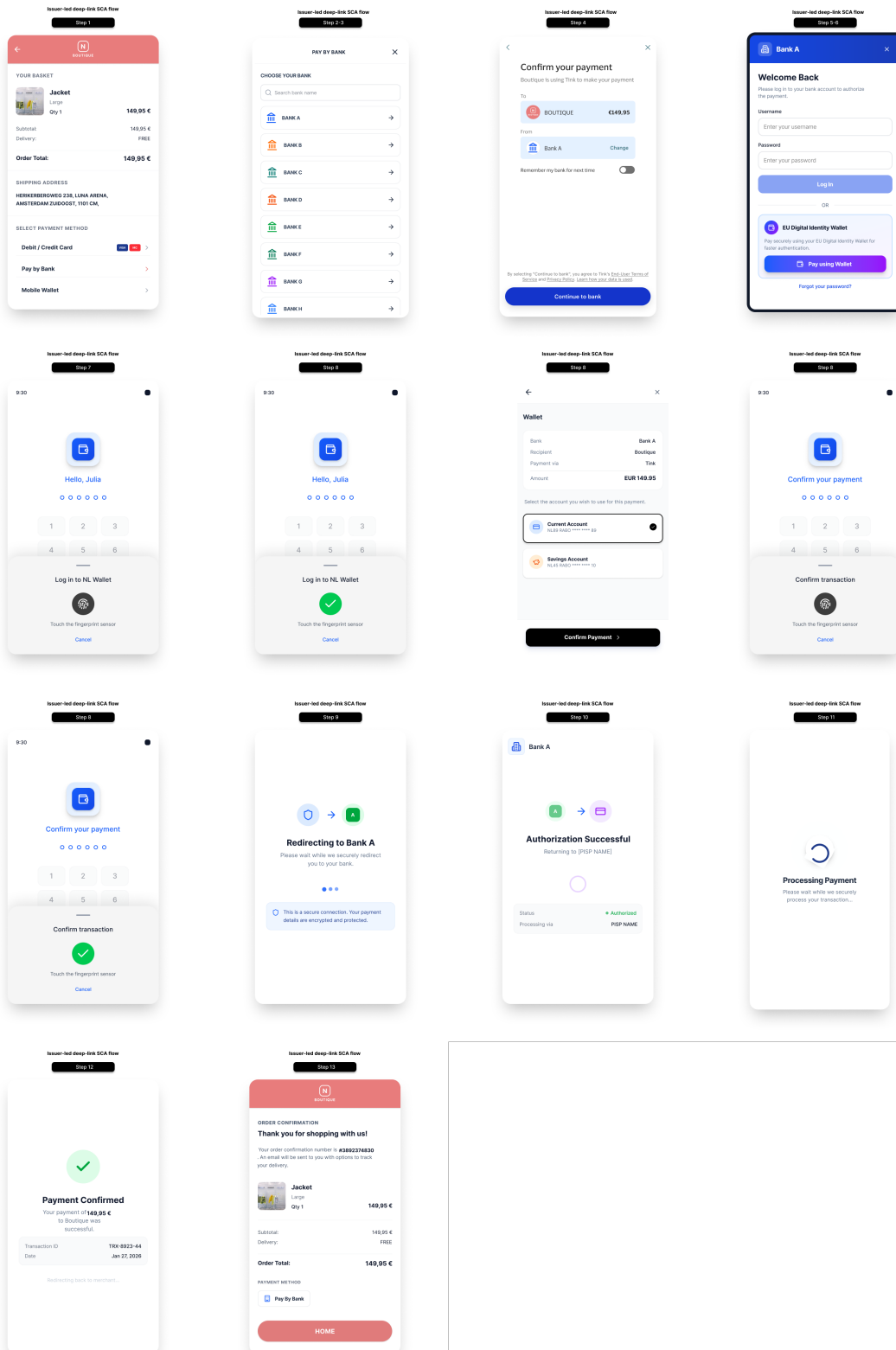
Dimension	Preferred	Alternative	What changes in the flow steps
Invocation mechanism	DC API (where supported)	Deep-link	DC API: OS handles selection/confirmation screen, wallet performs confirmation/presentation (wallet app may not open explicitly) Deep-link: wallet app opens; consumer unlocks wallet before confirmation/presentation.

2.2.1.5 UX/UI

DC API, SCA-IBAN same device



Deep-link, SCA-IBAN same device



2.3 Challenges and barriers

2.3.1 Wallet invocation mechanism maturity (DC API vs deep-link)

While W3C Digital Credential APIs (DC API) offer a more seamless and standardised wallet invocation experience, their practical availability depends on operating system support, browser capabilities and wallet provider maturity.

Deep-link invocation mechanisms are currently more widely supported and easier for banks to pilot, but may result in less consistent user experiences across platforms.

2.4 Working Assumptions

2.4.1 Issuer-requested SCA model

Scenario A1 assumes an **issuer-requested (bank-led) Strong Customer Authentication model**, where the bank remains the relying party for authentication during Open Banking A2A payment authorisation. Merchant-captured or PISP-captured SCA models are explicitly excluded from this scenario and are addressed under Scenario A2.

2.4.2 Scope limited to payment authentication only

Scenario A1 assumes that the use of the EU Digital Identity Wallet (EUDIW) is limited to **authentication for payment authorisation**. The wallet does not initiate or sign the payment itself and no payment execution logic is moved to the wallet. Existing Open Banking and SEPA payment processes remain unchanged.

2.4.3 No combined presentation in issuer-requested flows

It is assumed that **combined presentation of payment authentication with additional attributes** (e.g. age or other identity claims) is not supported in issuer-requested A1 flows. Supporting such combinations would require banks to relay wallet-provided attributes to merchants, which is considered out of scope due to complexity, unclear responsibilities and limited suitability for issuer-requested Open Banking patterns.

2.4.4 Attestation issuance as a pre-condition

It is assumed that SCA-IBAN attestations used in Scenario A1 are issued and verified by the same bank participating in PA2. Banks participating in Scenario A1 are also participating in PA1 Scenario 4 which defines and pilots issuance of SCA-IBAN attestation.

2.4.5 Optional wallet invocation mechanisms

It is assumed that wallet invocation mechanisms may vary across implementations. **W3C Digital Credential APIs (DC API)** are considered a preferred option where supported, while **deep-link** is assumed to be

available as fallback. No single invocation mechanism is assumed to be universally supported across all banks, devices or wallet providers.

Scenario A1 does not mandate support for specific mobile operating systems. Platform availability (e.g. Android, iOS) depends on wallet provider and invocation mechanism maturity and may vary between pilot partners.

2.4.6 Trust infrastructure availability

It is assumed that sufficient **trust infrastructure** (e.g. issuer trust lists and cryptographic verification material) is available to enable banks to verify wallet-presented SCA attestations. Where parts of this infrastructure are still evolving, temporary assumptions may be applied during piloting with the expectation of alignment to future EUDI ecosystem guidance.

2.4.7 Bank policy variability

Scenario A1 assumes that banks may apply **bank-specific policies** during payment authorisation (e.g. additional confirmation screens, account selection or supplementary checks), provided that the EUDIW-based SCA step is successfully completed. Such variations are considered acceptable within the scope of issuer-requested Open Banking flows.

3 Roles and participants

3.1 Roles represented in the scenario

The following roles are represented in Scenario A1. Roles and terminology are aligned with the PA2 Stock Taking phase and relevant ARF definitions.

Authentic Source / Issuer of SCA Attestation

- **Bank (ASPSP)**

The bank acts as the authentic source for SCA-IBAN attestations and issues these attestations to the user's EU Digital Identity Wallet outside of the payment flow.

Relying Party

- **Bank (ASPSP)**

In issuer-requested A2A SCA flows, the bank acts as the relying party and verifier of the SCA attestation it previously issued.

- The bank may rely on internal systems such as the Open Banking Interface (OBI), which provides the API layer for Open Banking flows.

Merchant

- Online merchant offering Account-to-Account (A2A) Pay-by-Bank payments via Open Banking.

Payment Initiation Service Provider (PISP)

- PISP facilitating Open Banking payment initiation and redirection between the merchant and the bank, where applicable.

Consumer

- Natural Person, existing consumer of the bank, using a Natural Person EU Digital Identity Wallet.

Wallet Provider

- Provider of the EU Digital Identity Wallet used by the holder for authentication.

Supporting ecosystem roles (not actively exercised in Scenario A1)

The following roles exist in the wider EUDI ecosystem but are not independently exercised in issuer-requested Scenario A1 flows:

- PID Provider
- Trusted List Registrar
- (Q)EAA / EAA / Pub-EAA / QES Providers

In Scenario A1, these roles do not independently request, issue, or verify credentials during the payment authentication flow.

3.2 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of EUDI Wallet	Consumers of one or more of the banks – National Bank of Greece (GR) – Komerční banka (CZ)	GR/CZ
2. Authentic sources / Issuer of SCA Attestation	Participating bank – National Bank of Greece (GR) – Komerční banka (CZ)	GR/CZ
3. Relying party	Participating bank – National Bank of Greece (GR) – Komerční banka (CZ)	GR/CZ
4. Merchant	– Cyclades Fast Ferries (EU) – Google (EU)	EU
5. Payment Initiation Service Provider	– Mastercard Open Banking Services EU (EU) – Tink (EU)	EU
6. EUDI Wallet Provider	– Aricoma (CZ)	CZ

3.3 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
--------------	-----------------	---------	--------

1. PID Provider	No additional scenario-specific requirements apply for this roles in Scenario A1. In issuer-requested A2A SCA flows, the bank acts as both the authentic source and the relying party for SCA attestations, and no third party independently requests or verifies wallet credentials. As a result, these roles are not actively exercised within Scenario A1 beyond their generic ecosystem responsibilities.
2. Trusted list registrar	
3. QEAA provider	
4. Pub-EAA provider	
5. EAA provider	
6. QES provider	

3.4 Target country combinations

	Issuing country						
Relying Party country		GR	CZ				
	GR		Yes				
	CZ	Yes					

3.5 Requirements

The main requirements for each of the involved roles are included as an Annex 1.

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.

Scenario A1 does not define or specify attestation issuance. The specification for issuance of SCA-IBAN attestation is developed under **PA1**, while the attestation specifications are defined in WP3 Technology&Standards.

For the PA2 pilot, however, **attestations used in Scenario A1 must be issued by a bank participating in PA2**, which also acts as the relying party during payment authentication.

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

Attestation name	Short description	To be provided by	For Countries	Requirements
SCA-IBAN Attestation	Payment-instrument SCA attestation used for account-based authentication and initiation scenarios.	WP3 T&S (attestation specification) PA1 (issuance specification) PA2 bank (issuance & verification)	Participating issuing bank countries	• Usable for issuer-requested Open Banking SCA where the bank is the relying party. • Bound to a specific IBAN to authenticate a concrete payment account. • Presentable via the EU Digital Identity Wallet (EUDIW) during payment authorisation. • Verifiable by the issuing bank under the WE BUILD trust framework. • Reusable across A.1 and A.2 scenarios. • If issued in PA1, the issuing bank MUST also participate in the PA2 pilot; otherwise SCA-IBAN MUST be issued by a PA2 bank.

4.3 Created attestations in the scenario

No attestations are created within Scenario A1.

The specification and issuance of SCA-IBAN attestations are handled outside this scenario. Scenario A1 only consumes existing attestations during issuer-led payment authentication.

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 have an active Natural Person EU Digital Identity Wallet installed and operational.
	b. Must be able to authenticate in the wallet using wallet-supported mechanisms (e.g. biometrics or PIN).
	c. Must explicitly consent to the use of the wallet for payment authentication.
2. Bank – Authentic Source, Issuer and Relying Party	a. Must support issuer-requested invocation of the EUDIW during Open Banking payment authorisation.
	b. Must be able to issue and verify SCA-IBAN attestations used in Scenario A1.
	c. Must verify wallet-presented attestations and bind the result to existing Open Banking payment flows.
3. Intermediary (PISP)	a. Must support standard Open Banking redirection and consent flows.
	b. Must not access or receive wallet credentials or attestations.
	c. Must relay authentication and payment outcomes according to existing Open Banking interfaces.
5. EUDI Wallet provider	a. Must support presentation of SCA-IBAN attestations.
	b. Must support wallet invocation via DC API and/or deep-link mechanisms.
	c. Must ensure user consent and clear presentation of the SCA request.
6. Merchant	a. Must support Open Banking Pay-by-Bank payments, either directly or via a PISP.
	b. Must not interact directly with the EU Digital Identity Wallet.
	c. Must display the payment outcome to the user based on the bank/PISP response.
	d. Must not rely on wallet-based authentication signals for authorisation decisions; payment confirmation remains based solely on Open Banking payment outcome.
7. PID Provider	No additional scenario-specific requirements apply for this roles in Scenario A1. In issuer-requested A2A SCA flows, the bank acts as both the authentic source and the relying party for SCA attestations, and no third party independently requests or verifies wallet credentials. As a result, these roles are not actively exercised within Scenario A1 beyond their generic ecosystem responsibilities.
8. Trusted list registrar	
9. QEAA provider	
10. Pub-EAA provider	
11. EAA provider	
12. QES provider	

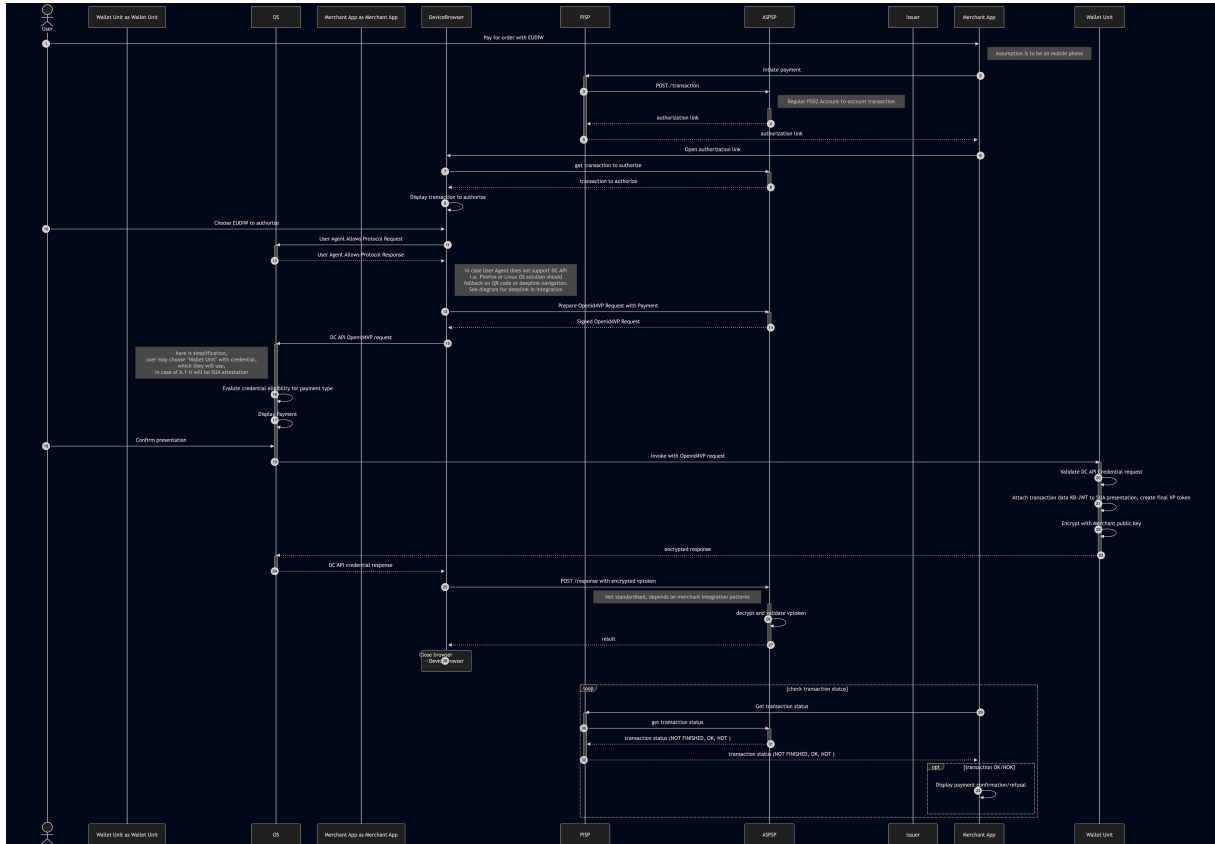
Annex 2 – Sequence Diagrams

Note: For the most up to date version on WE BUILD GitHub <https://github.com/webuild-consortium/wp3-technology-standards/tree/main/PA2> (private access, invites only)

Deep-link



DC API



WE BUILD consortium

MVP Specification

Scenario A.2 – A2A

Payment Initiation

WP3 – PA2 Consumer payments

Date : 2026-06-18
Version : 1.0
Status : For review

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>	5
2.4	<i>Scenario additional flows.....</i>	6
2.5	<i>Challenges and barriers</i>	7
2.6	<i>Working Assumptions</i>	8
3	Detailed scenario flow.....	10
3.1	<i>UX Flows</i>	13
3.1.1	<i>DC API same device flow</i>	13
3.1.2	<i>DC API cross device flow</i>	14
3.1.3	<i>Same device Custom URI fallback flow</i>	14
3.1.4	<i>Cross device Custom URI fallback flow</i>	15
4	Roles and participants.....	17
4.1	<i>Scenario roles and participants.....</i>	17
4.2	<i>Additional roles and partners</i>	17
4.3	<i>Target country combinations.....</i>	17
4.4	<i>Requirements.....</i>	17
5	Attestations	18
5.1	<i>Introduction</i>	18
5.2	<i>Attestations to be provided by other UCs/WGs/scenarios</i>	18
5.3	<i>Created attestations in the scenario.....</i>	18
	Annex 1 – Requirements for scenario roles.....	19
	Annex 2 – Technical diagrams and examples	23
	DC API flow	23
	Deep-Link API flow (same device and cross device).....	23
	Technical request examples	24

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario A2A Payment Initiation, as part of use case PA2 in WP3 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 pilots cross-border Account-to-Account (A2A) payment initiation using the EU Digital Identity Wallet (EUDIW), where a holder presents an SCA-IBAN attestation issued by their ASPSP (bank) to authenticate and authorize payments at an online merchant's checkout, leveraging OpenID4VP and the W3C Digital Credential API (with Custom URI alternative as a fallback) for secure, wallet-based transaction signing.

It is part of a wider set of scenarios that have been developed in PA2:

- A1 Account-based online payment SCA with the EUDIW
- A2 Account-based payment initiation with the EUDIW
- B1 Card-based online payment SCA with the EUDIW
- B2 Card-based payment initiation with the EUDIW

The scenario is based on the following documentation:

• Technology / Specification	• Publication URL
• ARF v2.9	• https://eudi.dev/2.9.0/
• ARF Technical Specification 12 v1.0.1	• https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts12-electronic-payments-SCA-implementation-with-wallet.md
• W3C Digital Credentials API	• https://www.w3.org/TR/digital-credentials/
• PSD2 (Directive (EU) 2015/2366)	• https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
• Regulation on SCA (Recital 62 and Article 5f2)	• https://eur-lex.europa.eu/eli/reg/2024/1183/oj

• WE BUILD WP3 PA2 Stock Taking 1.01	• WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=5920&fid%5B0%5D=201&fid%5B1%5D=202&fid%5B2%5D=4208
• SD-JWT VC (IETF draft)	• https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/
• OID4VCI 1.0	• https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
• VP 1.0	• https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
• W3C Verifiable Credentials Data Model	• https://www.w3.org/TR/vc-data-model/

2 Scenario specification

2.1 Introduction

This scenario covers the Account to Account (A2A) payment initiation method where a customer selects 'Pay with EU Digital Identity Wallet' option on merchants checkout page with an optional combined presentation with Loyalty card and/or Student card. Payment flows developed using W3C Digital Credential APIs standard or Custom URI and native OpenID4VP/VCI variants.

2.2 Scenario pre-conditions

Pre-conditions:

- Holder has an EU Digital Identity Wallet app on their phone.
- Holder has completed their account registration on EUDIW app and as such a PID has been successfully issued in the EU Digital Identity Wallet app of the Holder.
- Holder's EU Digital Identity Wallet has been onboarded into Holder's bank in PA1 scenario.
- Holder has SCA-IBAN attestation available in their Wallet.
- Holder has optionally either Loyalty Card or Student Card in their Wallet.
- Bank has a new API for accepting Signed Transaction Request.
- Merchant (or PISP) that is being used by the Merchant has to be a registered Relying Party in EUDI ecosystem.
- PISP needs a PISP license as TPP in the bank.
- PISP needs to have a new API from the bank implemented.

2.3 Scenario main flow

1. Holder goes to Merchant to buy goods or services, and add items into their basket
2. At checkout, they choose "Pay with EU Digital Identity Wallet" among other payment options.
3. The EU Digital Identity Wallet app is triggered by Merchant (or PISP on behalf of Merchant) using DC API or Custom URI where user authorises the payment details.
4. The SCA-IBAN is used to sign payment data with IBAN attestation and sent to merchant.
5. Merchant (or PISP) sends the data to banks' API to process Signed Transaction Request.

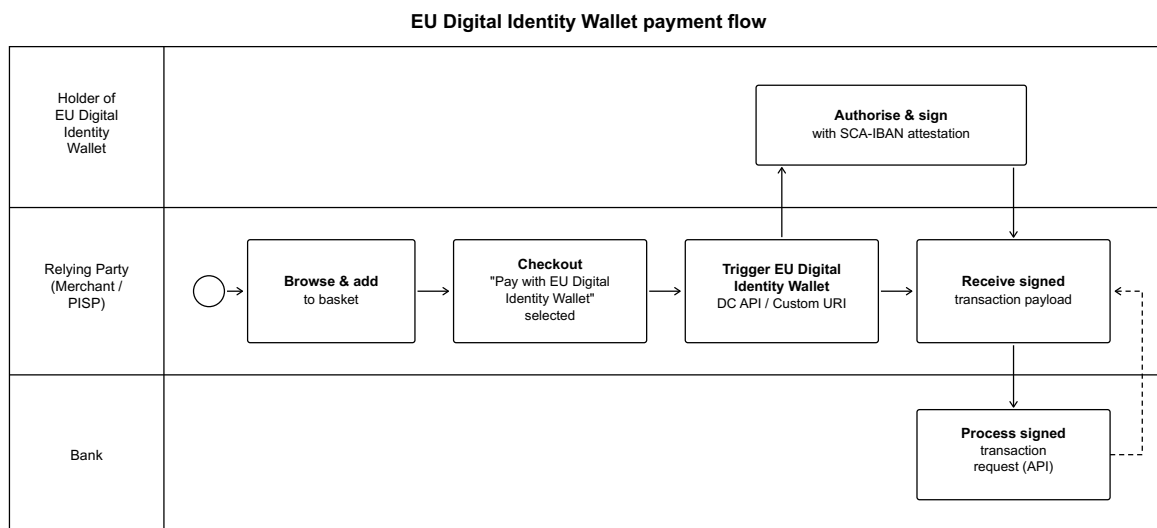


Figure 1: Scenario main flow

2.4 Scenario additional flows

Flow	Short description
Variations	
- Same device Custom URI flow	The payment initiation is executed on a single device where the merchant's checkout page triggers the holder's EUDIW directly via a Custom URI Deep Link (app-to-app). The holder's browser redirects to the wallet app, which presents the SCA-IBAN attestation and returns the signed VP back to the merchant's checkout via a callback URI, without relying on the W3C Digital Credential API.
- Cross device Custom URI flow	The merchant's checkout is accessed on one device (e.g. desktop browser) while the holder's EUDIW resides on a separate device (e.g. mobile phone). The merchant displays a QR code or deep link that the holder scans or opens on their mobile device to trigger the wallet. The signed VP is returned to the merchant session via a back-channel or redirect mechanism.
- Cross device DC API flow	The payment initiation is executed across two devices where the merchant's checkout page uses the W3C Digital Credential API on the primary device (e.g. desktop browser) to initiate a cross-device wallet interaction. The DC API handles the handover to the holder's mobile EUDIW, which presents the SCA-IBAN attestation and returns the signed VP back to the merchant session.
- Optional additional credentials for combined presentation	The Merchant's checkout page will require optional credentials, either Loyalty Card or Student Card for combined presentation by the Wallet alongside the SCA-IBAN attestation.
Exceptions	
- IBAN attestation not present in wallet	The holder attempts to initiate payment but has not yet registered an SCA-IBAN attestation in their EUDIW. The wallet or merchant checkout displays an appropriate error and guides the holder to first complete SCA-IBAN issuance via their bank (PA1 pre-requisite flow).
- IBAN attestation expired or revoked	The holder's SCA-IBAN attestation is present in the wallet but has expired or been revoked (e.g. account closed). The merchant or PSP rejects the signed transaction request and the holder is prompted to re-issue or update their attestation.

- Payment declined by bank	The signed transaction request is submitted to the bank API but the bank declines (e.g. insufficient funds, fraud detection). The merchant receives a decline response and informs the holder to choose an alternative payment method.
- User aborts wallet presentation	The holder chooses not to consent to the wallet presentation at checkout (e.g. cancels the EUDIW prompt). The checkout session returns to the payment selection page without completing the transaction.

2.5 Challenges and barriers

The following main challenges and barriers are anticipated for the development and piloting of the PA2 A2A Payment Initiation scenario:

- 1. Industry standardization of the SCA-IBAN Attestation:** No agreed EU-wide schema or rulebook for an IBAN attestation currently exists under eIDAS2/ARF. Piloting requires scenario partners to define and align on a fit-for-pilot attestation format, which may need revision as ARF guidance matures. Coordination with WP4 SEMANTICS is essential.
- 2. Bank API Readiness (Signed Transaction Request):** The scenario depends on banks exposing a new API capable of accepting and processing a Signed Transaction Request carrying SCA-IBAN attestation data. Many bank partners do not yet have this infrastructure. Building or adapting this API is a significant technical and regulatory effort, particularly for smaller or legacy banking institutions. Scenario Leads are in talks with the Czech Banking Association to incorporate it into their OpenBanking stack and afterwards it will be forwarded into Berlin Group and other OpenBaking groups.
- 3. Cross-Border Interoperability:** The scenario involves issuers (banks) and relying parties (merchants) located in different countries. Ensuring that an SCA-IBAN attestation issued by a bank in one country is accepted and verifiable by a merchant and PSP in another country requires cross-border trust framework alignment, trusted list recognition, and consistent schema interpretation.
- 4. Integration with Existing Payment Infrastructure:** Merchants and PISPs operate existing payment stacks (e.g. acquiring networks, 3DS, open banking flows). Integrating EUDIW-based A2A payment initiation alongside or into these stacks without disrupting existing checkout UX may technically complex and requires cooperation from shopping cart vendors and PSPs.
- 5. W3C Digital Credential API Maturity:** The scenario aims to pilot both W3C DC API-based and Custom URI/OpenID4VP native flows. The W3C DC API is still evolving and browser/OS support is not yet universal, creating uncertainty for same-device web checkout implementations.
- 6. User Consent and Data Minimization:** For the combined presentation flows (e.g. payment + Loyalty Card), ensuring that selective disclosure is implemented correctly and that holders

are clearly informed of what data they are sharing introduces both technical (ZKP or selective disclosure) and UX design challenges.

7. Liability and Legal Framework: The legal accountability for failed or disputed payments initiated via EUDIW (as opposed to traditional PSD2 flows) is not yet clearly defined. It is unclear how existing payment regulation (PSD2/PSR) maps to EUDIW-initiated payment flows, creating uncertainty for bank and merchant partners.

8. Immaturity and Instability of Payment Technical Specifications (TS12): The Technical Specification covering payments (TS12) is still not finalized and is expected to evolve significantly during the pilot development period. There is a risk that key design decisions made in this scenario — such as the structure of the Signed Transaction Request, the IBAN attestation format, or the wallet invocation mechanism — may need to be substantially revised or even redesigned if TS12 undergoes major changes. This creates uncertainty for scenario partners investing in development ahead of specification stability, and close monitoring of TS12 progress will be required throughout the project lifecycle.

2.6 Working Assumptions

The following working assumptions are established to provide a stable development foundation for the scenario, pending further guidance from ARF, EBA, and relevant standardization bodies:

WA-1: SCA-IBAN Attestation Format Assumption: The scenario will use a fit-for-pilot SCA-IBAN attestation in SD-JWT VC format designed by WP3 Technology and Standards group (aligned with ARF v2.x attestation requirements), including at minimum: subject, masked IBAN, , currency, and issuing bank identifier. This format is assumed to be adoptable by future ARF versions. *Trigger for revision:* If ARF or EBA publish a normative SCA-IBAN attestation schema prior to piloting that differs materially, scenario partners will align to that schema.

WA-2: Signed Transaction Request Assumption: The mechanism for the holder signing payment data using their EUDIW (binding the payment to the SCA-IBAN attestation) will follow an OpenID4VP SD-JWT profiled presentation where the transaction details are included in the presentation request nonce or transaction_data field, per emerging ARF guidance on transaction data binding. *Trigger for revision:* If the ARF adopts a different mechanism for transaction authorization within EUDIW, this assumption will be revisited.

WA-3: W3C DC API as Primary Same-Device Flow Assumption: The same-device web checkout flow will target the W3C Digital Credential API as the primary invocation mechanism, with Custom URI/native OpenID4VP as a fallback where DC API is not supported. Browser and OS support (Chrome, Android) is assumed to be sufficiently available in the pilot timeframe. For pilot purpose Android device will be used

WA-4: PA1 SCA-IBAN Issuance as Pre-Condition Assumption: The issuance of the SCA-IBAN attestation into the EUDIW (PA1 scenario 4) is treated as a fulfilled pre-condition for PA2. PA2 development will not re-specify the issuance flow but will rely on the SCA-IBAN

attestation being present and valid in the wallet at the start of the payment flow. Banks that wants to pilot this scenario requires to be part of scenario PA1 and PA2.

WA-5: PSD2/PSR Compliance *Assumption:* The EUDIW-based A2A payment initiation is treated as an 3rd party captured strong customer authentication (SCA) mechanism compatible with PSD2/PSR requirements. Banks implementing the Signed Transaction Request API are assumed to take responsibility for regulatory compliance on their side. The scenario will not attempt to resolve open PSD2/PSR interpretations but will flag these as a barrier.

WA-6: Commercial Terms for Signed Transaction Request API *Assumption:* The bank API for accepting Signed Transaction Requests is not mandated under PSD2/PSR open banking obligations, and banks may therefore charge for access to this API at their own discretion. The commercial arrangements between banks, PSPs, and merchants for API access are outside the scope of this scenario and will not be defined, negotiated, or covered within the pilot. Scenario partners are expected to resolve any applicable API access fees bilaterally. *Trigger for revision:* If future PSD2/PSR or EBA guidance mandates free or regulated access to such APIs, this assumption will be revisited.

WA-7: EUR Currency for Pilot Transactions *Assumption:* All PISPs and banks participating in the pilot will process A2A payment transactions exclusively in EUR currency. Multi-currency support, foreign exchange handling, and non-EUR account scenarios are out of scope for this pilot. *Trigger for revision:* If pilot partners require support for additional currencies, this assumption will be revisited and the scope adjusted accordingly.

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
Step 1: Holder selects items and proceeds to checkout	Holder (incl. wallet)	The holder browses the online merchant's website, adds items to the basket, and navigates to the checkout page. No wallet interaction yet.		
Step 2: Merchant presents payment options	Relying Party (Merchant)	The merchant's checkout page renders available payment methods, including a "Pay with your EUDIW [wallet name]" option alongside traditional methods (card, bank transfer, etc.) with option to provide additional credentials like Loyalty Card or Student Card.	Merchant checkout integration with EUDIW payment option (shopping cart vendor).	If EUDIW option is not available, holder falls back to traditional payment.
Step 3: Holder selects "Pay with EUDIW"	Holder	The holder taps/clicks the EUDIW payment option. The merchant prepares a payment request including transaction details (amount, currency, merchant ID, reference) and sends it to PISP		Holder may abort here; exception: user cancels flow.
Step 4: Merchant/PSP constructs OpenID4VP presentation request	Relying Party (Merchant)	The PISP constructs an OpenID4VP Presentation Request, including transaction data as per TS12 (amount, payee, reference) in the request. The request specifies the SCA-		

		IBAN attestation as the required credential with required selectively disclosable fields and optionally additional credentials, Request is returned to Merchant		
Step 5: EUDIW app is triggered via DC API or Custom URI	Holder	The merchant's checkout page triggers the holder's EUDIW using the W3C Digital Credential API (same-device or browser-to-app) or a Custom URI scheme as fallback. The wallet receives the presentation request.	W3C DC API browser support; wallet provider DC API implementation.	Exception: wallet not installed — merchant prompts holder to install.
Step 6: Wallet displays transaction details and requests holder consent	Holder	The EUDIW app parses the presentation request and displays the transaction details (amount, payee, purpose) to the holder. The holder is prompted to review and authorise the payment by consenting to present their SCA-IBAN attestation and optionally additional credentials.	Wallet provider UX implementation; SCA-IBAN attestation present in wallet (PA1 pre-condition). Display of transaction data according TS12 by Wallet	Exception: SCA-IBAN attestation not found in wallet or additional credentials are not available — wallet displays error and prompts holder to first register bank account or additional required credentials. Exception: attestation expired/revoked — wallet notifies holder.
Step 7: Holder authenticates and authorises within EUDIW	Holder	The holder authenticates within the wallet (PIN, biometric) and confirms consent to present the SCA-IBAN attestation and optionally additional	Wallet provider authentication mechanism.	

		credentials and sign the transaction data hashes.		
Step 8: EUDIW generates and returns signed presentation (VP)	Holder	The EUDIW creates a Verifiable Presentation (VP) containing the SCA-IBAN attestation (SD-JWT VC) with transaction data binding (signed with the holder's key over the transaction data hash). The encrypted VP token is returned to the merchant via the DC API response or Custom URI callback.	ARF-compliant VP format; OpenID4VP response handling by merchant/PISP.	
Step 9: Merchant/PSP verifies the VP and extracts payment credentials	Relying Party (Merchant)	The merchant passes VP token to PISP and PISP decrypts and verifies the VP: validates the attestation signature (against issuer certificate on trusted list), verifies the transaction data hash binding, and extracts the SCA-IBAN and holder details.	Trusted list access; attestation schema; PISP verification capability.	Exception: VP verification fails (invalid signature, untrusted issuer) — merchant rejects payment and notifies holder.
Step 10: Merchant/PSP sends Signed Transaction Request to bank API	Relying Party (Merchant)	The PISP constructs and submits a Signed Transaction Request to the bank's API, including the verified IBAN, transaction details, and the VP as evidence of holder authorisation.	Bank's new Signed Transaction Request API (pre-condition).	Exception: bank API unavailable — merchant displays error, holder prompted to retry or use alternative payment.
Step 11: Bank processes payment and returns result	EAA Provider (Bank as Authentic Source /	The bank validates the Signed Transaction Request, checks the account (funds, status), and initiates the A2A	Bank internal payment processing; A2A credit transfer infrastructure.	Exception: payment declined (insufficient funds, fraud) — merchant

	Issuer)	credit transfer. The bank returns a payment confirmation or decline response to the PISP.		informs holder.
Step 12: Merchant confirms order to holder	Relying Party (Merchant)	Upon receiving payment confirmation from the PISP, the merchant's checkout page displays a payment success confirmation and order summary to the holder.		Exception: payment declined — merchant shows failure message and offers alternative payment methods.

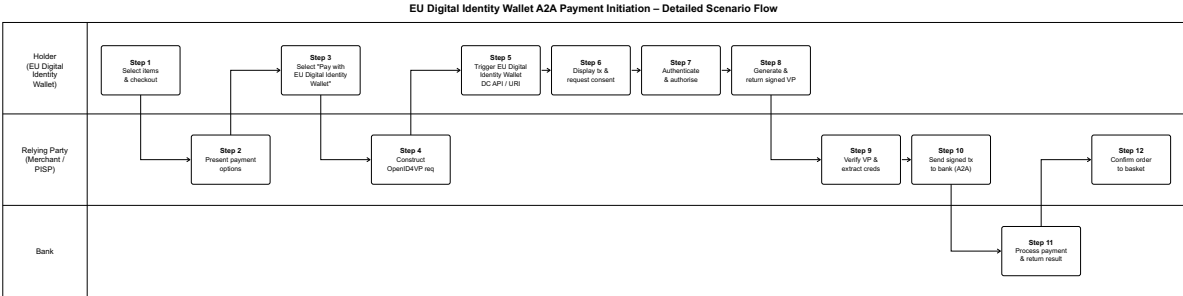


Figure 2: Detailed Scenario Flow

3.1 UX Flows

3.1.1 DC API same device flow

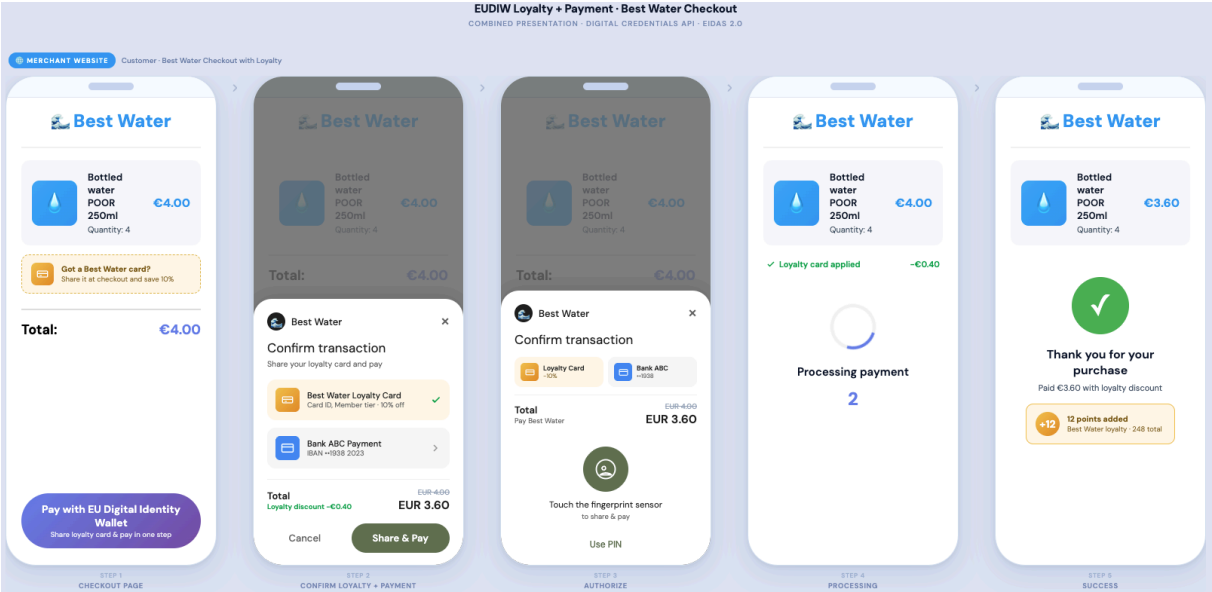


Figure 3: The UX flow shows a possibility of a combined presentation sharing of the Loyalty Card attestation and using SCA-IBAN attestation.

3.1.2 DC API cross device flow

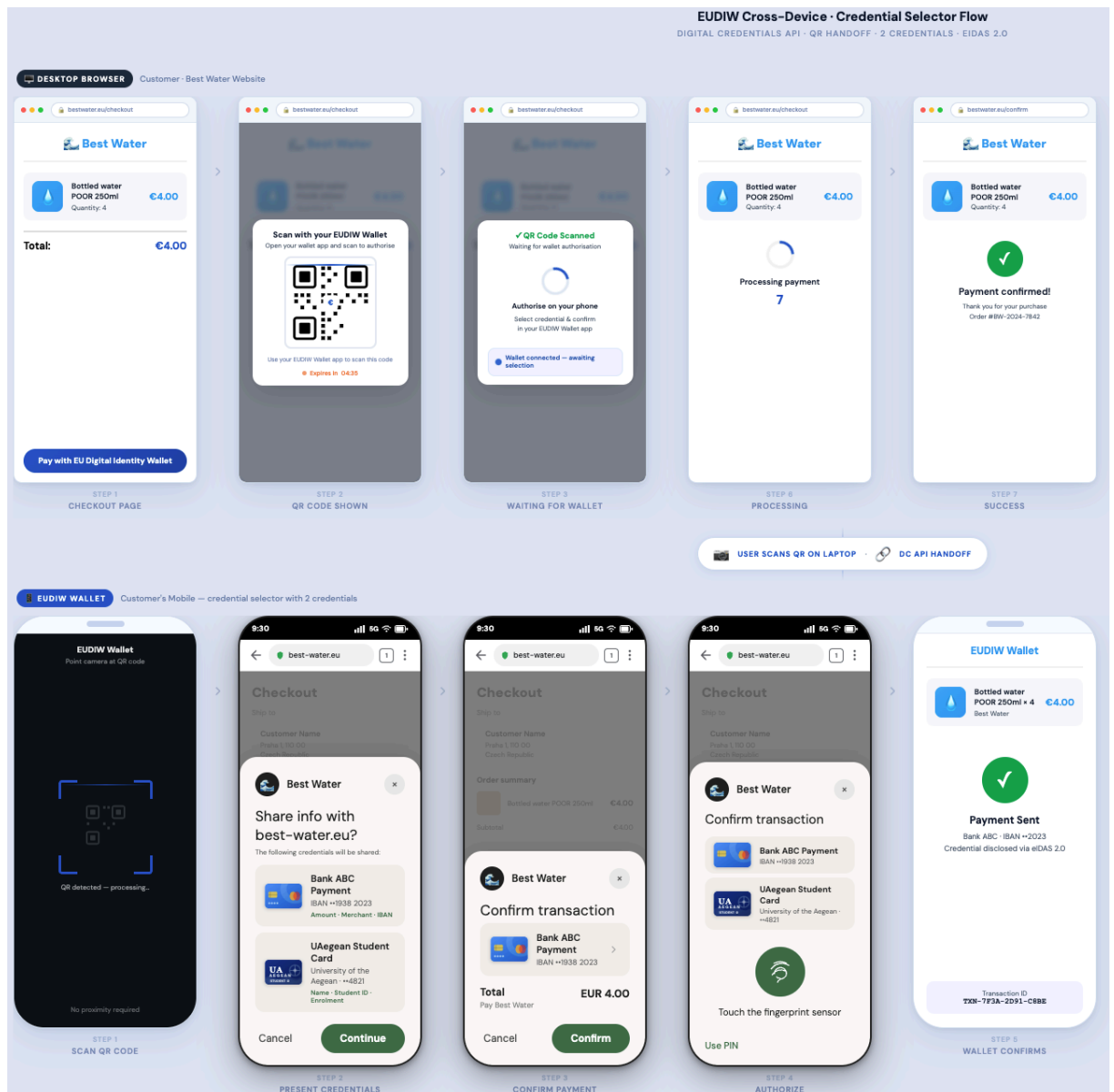


Figure 4: The UX flow shows a possibility of a using SCA-IBAN attestation for payment initiation for a cross device scenario without combined presentation.

3.1.3 Same device Custom URI fallback flow

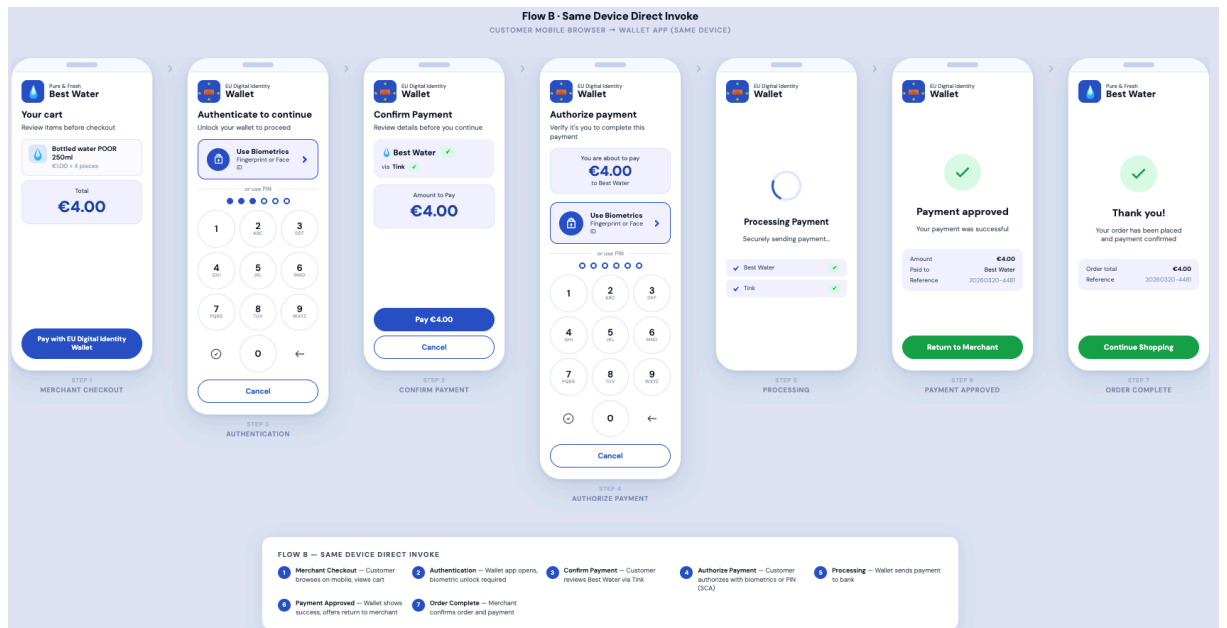


Figure 5: The UX flow shows a possibility of a using SCA-IBAN attestation for payment initiation for a same device scenario with Custom URI/Deeplink without combined presentation.

3.1.4 Cross device Custom URI fallback flow

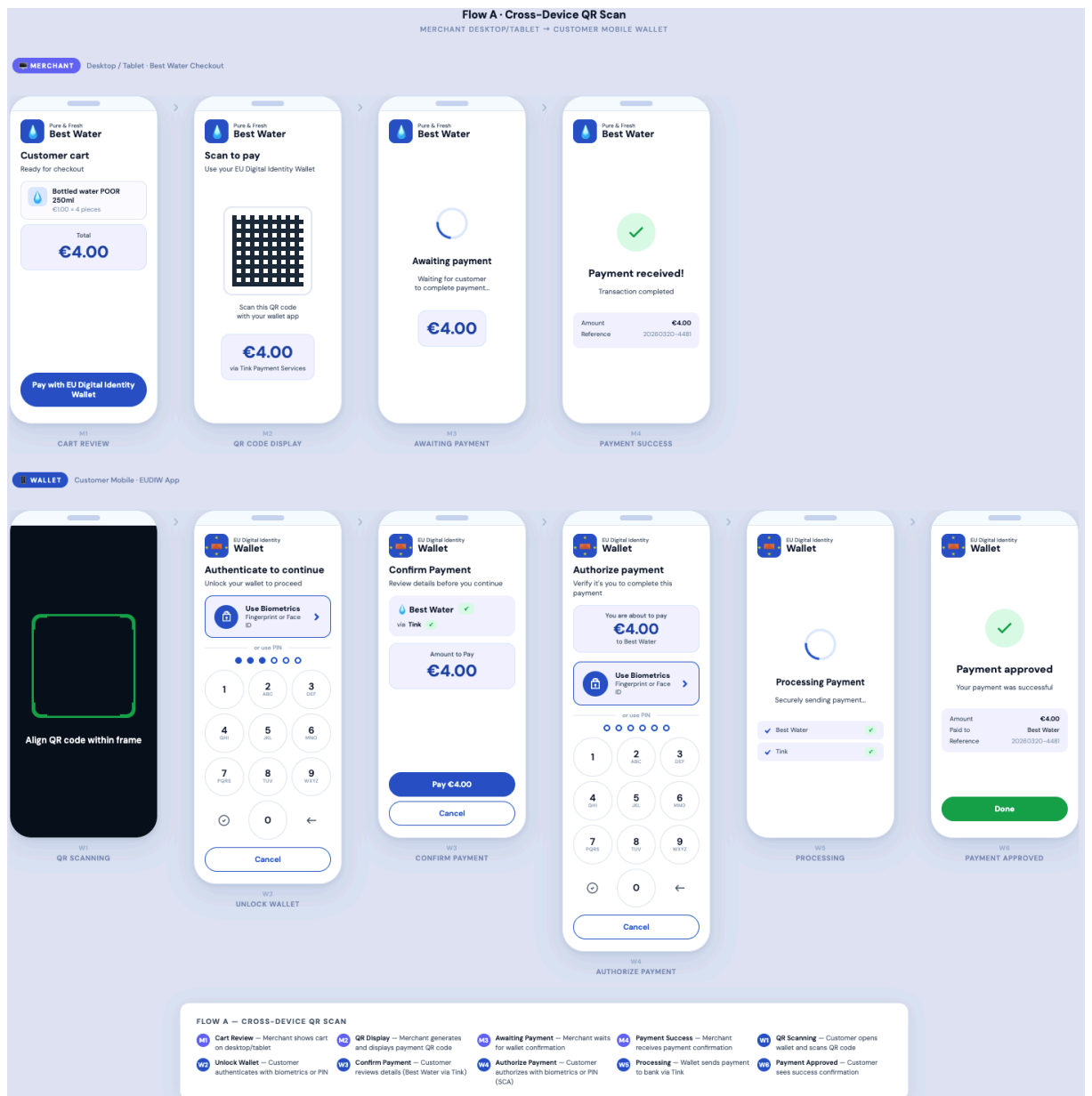


Figure 6: The UX flow shows a possibility of a using SCA-IBAN attestation for payment initiation for a cross device scenario with Custom URI/Deeplink without combined presentation.

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of EUDI Wallet	Air Bank, a.s.	CZ
	Komerční banka, a.s.	CZ
2. Authentic sources	Air Bank, a.s.	CZ
	Komerční banka, a.s.	CZ
	Fast Ferries (Issuer)	GR
3. Relying party	Fast Ferries (Merchant)	GR
	Google (Merchant)	IR
4. Intermediary	UAegean	GR

4.2 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	ARICOMA	CZ	RW
	IGrant.io	SW	NW
2. PID Provider	GRNET	GR	
	ARICOMA	CZ	
3. EAA provider	Bank iD CZ	CZ	
	Fast Ferries	GR	
4. PISP	Google	IR	
	Worldline	FR	

4.3 Target country combinations

Relying Party country	Issuing country						
		AT	BE	DE	FI	GR	CZ
	AT						
	BE						
	DE						
	FI						
	GR						X
	CZ					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
SCA- IBAN	SUA Attestation according TS12 specification containing also information about IBAN	PA1	CZ	
Student Card	Student loyalty card from university of Aegean	WP3 T&S	GR	
Loyalty Card	Loyalty Card from Fast Ferries	WP3 T&S	GR	

5.3 Created attestations in the scenario

No attestation will be created in this scenario.

Annex 1 – Requirements for scenario roles

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

Primary role	Priority	Specific requirement
User of EUDI Wallet	Must Have	Holder has an active EUDIW installed on an Android device.
	Must Have	Holder has a valid PID issued into their EUDIW (required for wallet activation per WE BUILD Blueprint).
	Must Have	Holder has a valid SCA-IBAN attestation (SD-JWT VC) issued via PA1 installed in their EUDIW prior to initiating payment.
	Must Have	Holder is able to authenticate within the wallet using PIN or biometric to authorise transaction signing.
	Must Have	Holder's wallet supports explicit, transparent consent before releasing any attestation (no auto-consent per WBCS Credential Presentation).
	Should Have	Holder optionally has a Loyalty Card or Student Card attestation available in their EUDIW for combined presentation flows.
	Should Have	Holder understands what data is being shared at checkout (clear wallet UX per Blueprint selective disclosure requirements).
	Could Have	Holder is able to use the same EUDIW for both same-device (DC API) and cross-device (QR/Custom URI) checkout scenarios.
	Won't Have	Holder is not required to have a QES capability in their wallet for this pilot.
Relying Party (Merchant)	Must Have	Merchant has integrated a "Pay with your EUDIW" option into their online checkout page alongside existing payment methods.
	Must Have	Merchant or their PISP is registered as a Relying Party in the WE BUILD ecosystem and holds a valid WE BUILD RP access certificate.
	Must Have	Merchant supports invocation of the EUDIW via W3C Digital Credential API (DC API) as the primary same-device mechanism.
	Must Have	Merchant (or PISP on their behalf) constructs a valid OpenID4VP Presentation Request including transaction data fields as specified in TS12.
	Must Have	Merchant (or PISP) implements the Presentation Request Object as a signed, integrity-protected object per WBCS Credential Presentation requirements.
	Must Have	Merchant (or PISP) validates the VP response, including attestation signature, transaction data hash binding, WUA validity, and SD-JWT VC disclosure integrity.
	Should Have	Merchant supports Custom URI / Deep Link as a fallback invocation mechanism for same-device and cross-device flows.
	Should Have	Merchant supports optional combined presentation (requesting Loyalty Card or Student Card alongside SCA-IBAN) in the checkout request.

Primary role	Priority	Specific requirement
Intermediary (PISP)	Should Have	Merchant provides clear feedback to the Holder upon payment success or failure.
	Could Have	Merchant supports cross-device DC API flow (QR code-based wallet invocation on desktop).
	Won't Have	Merchant is not required to directly access the bank API; this is handled via PISP in this scenario.
	Must Have	PISP holds a valid PISP licence as a Third Party Provider (TPP) authorised under PSD2/PSR.
	Must Have	PISP is registered as a Relying Party in the WE BUILD ecosystem with a valid WE BUILD RP access certificate.
	Must Have	PISP constructs the OpenID4VP Presentation Request per TS12, embedding transaction data (amount, payee, currency, reference) in the transaction_data field.
	Must Have	PISP verifies the returned VP: validates the attestation signature against the issuer certificate on the WE BUILD Trusted List, checks transaction data hash binding, and extracts the IBAN.
	Must Have	PISP constructs and submits a Signed Transaction Request to the bank's API including the verified IBAN, transaction details, and VP evidence.
	Must Have	PISP has integrated the bank's new Signed Transaction Request API (pre-condition per WA-4).
	Must Have	PISP processes transactions exclusively in EUR currency (per WA-7).
	Should Have	PISP supports nonce and audience validation per WBCS Credential Presentation (nonce and audience restrictions generated per transaction).
	Should Have	PISP provides a Presentation Response Endpoint per WBCS Credential Presentation.
	Should Have	PISP publishes Verifier Metadata per WBCS Credential Presentation deployment requirements.
	Could Have	PISP supports combined presentation verification (SCA-IBAN + Loyalty Card or Student Card).
	Won't Have	PISP is not required to support multi-currency processing in this pilot (per WA-7).
EUDI Wallet Provider	Must Have	Wallet provider delivers a EUDIW that passes WE BUILD ITB testing prior to pilot participation.
	Must Have	Wallet supports HAIP-compliant OpenID4VP per WBCS Credential Presentation requirements.
	Must Have	Wallet supports same-device and cross-device presentation flows (WBCS Credential Presentation 7.1.2).
	Must Have	Wallet supports the openid4vp://present invocation scheme (WBCS 7.1.3).
	Must Have	Wallet validates signed Presentation Request Objects and rejects unsigned or invalid requests (WBCS 7.1.4).

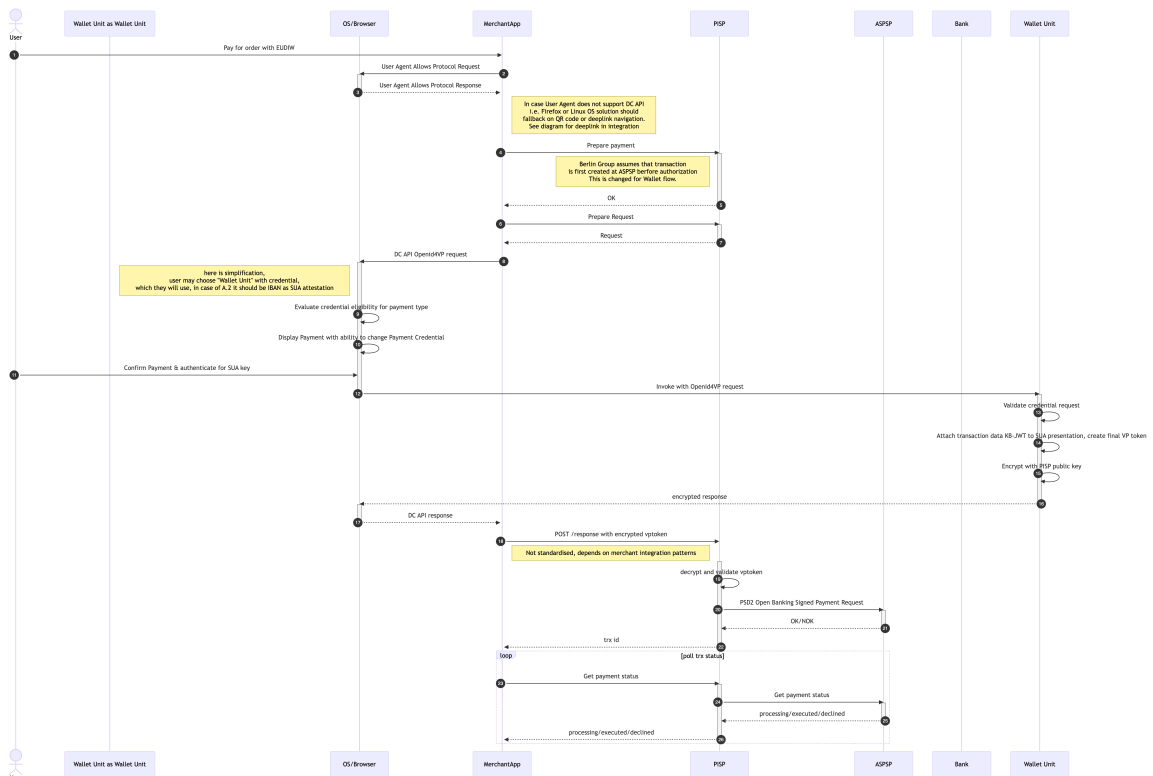
Primary role	Priority	Specific requirement
PID Provider	Must Have	Wallet implements SD-JWT VC selective disclosure for the SCA-IBAN attestation (WBCS 7.1.5).
	Must Have	Wallet displays transaction data to the Holder as required by TS12 before requesting consent.
	Must Have	Wallet generates a JWT-based Presentation Proof bound to the Verifier's nonce and audience (WBCS 7.1.7–7.1.8).
	Must Have	Wallet supports DC API invocation on Android (per WA-3).
	Must Have	Wallet supports revocation checking for attestations (Blueprint section 6.3).
	Should Have	Wallet supports Custom URI / Deep Link as a fallback invocation mechanism.
	Should Have	Wallet supports combined presentation of multiple credentials in a single VP.
	Could Have	Wallet supports cross-device DC API flow.
	Won't Have	Wallet is not required to support ISO 18013-5 mdoc format for this scenario (SD-JWT VC only per WA-1 and WBCS CS01_01).
	Must Have	PID Provider can issue a valid PID in SD-JWT VC format into the EUDIW using OID4VCI per WBCS Credential Issuance.
EAA Provider (Bank)	Must Have	PID Provider is registered on the WE BUILD Trusted List.
	Must Have	PID Provider supports wallet activation (PID is a pre-condition for EUDIW activation per Blueprint).
	Should Have	PID Provider supports revocation of PID attestations (Blueprint section 6.3).
	Won't Have	PID Provider is not required to participate directly in payment flows; PID is only needed for wallet activation.
	Must Have	Bank issues valid SCA-IBAN attestations in SD-JWT VC format into the Holder's EUDIW via OID4VCI per WBCS Credential Issuance (delivered through PA1).
	Must Have	Bank exposes a new Signed Transaction Request API capable of accepting and processing the VP-based payment authorisation submitted by the PISP.
	Must Have	Bank is registered on the WE BUILD Trusted List as an EAA provider to enable cross-border verification of SCA-IBAN attestations.
	Must Have	Bank processes A2A credit transfers in EUR upon successful Signed Transaction Request validation (per WA-7).
	Must Have	Bank supports attestation revocation (e.g. when an account is closed) per Blueprint section 6.3.
	Must Have	Bank participates in both PA1 (SCA-IBAN issuance) and PA2 (payment initiation) scenarios (per WA-4).
	Should Have	Bank returns clear payment confirmation or decline responses to the PISP with standardised error codes.

Primary role	Priority	Specific requirement
	Could Have	Bank's Signed Transaction Request API is aligned with or contributed to the Berlin Group / Czech Banking Association OpenBanking stack for broader interoperability.
	Won't Have	Bank is not required to provide free access to the Signed Transaction Request API; commercial terms are resolved bilaterally (per WA-6).
	Won't Have	Bank is not required to process non-EUR transactions in this pilot (per WA-7).

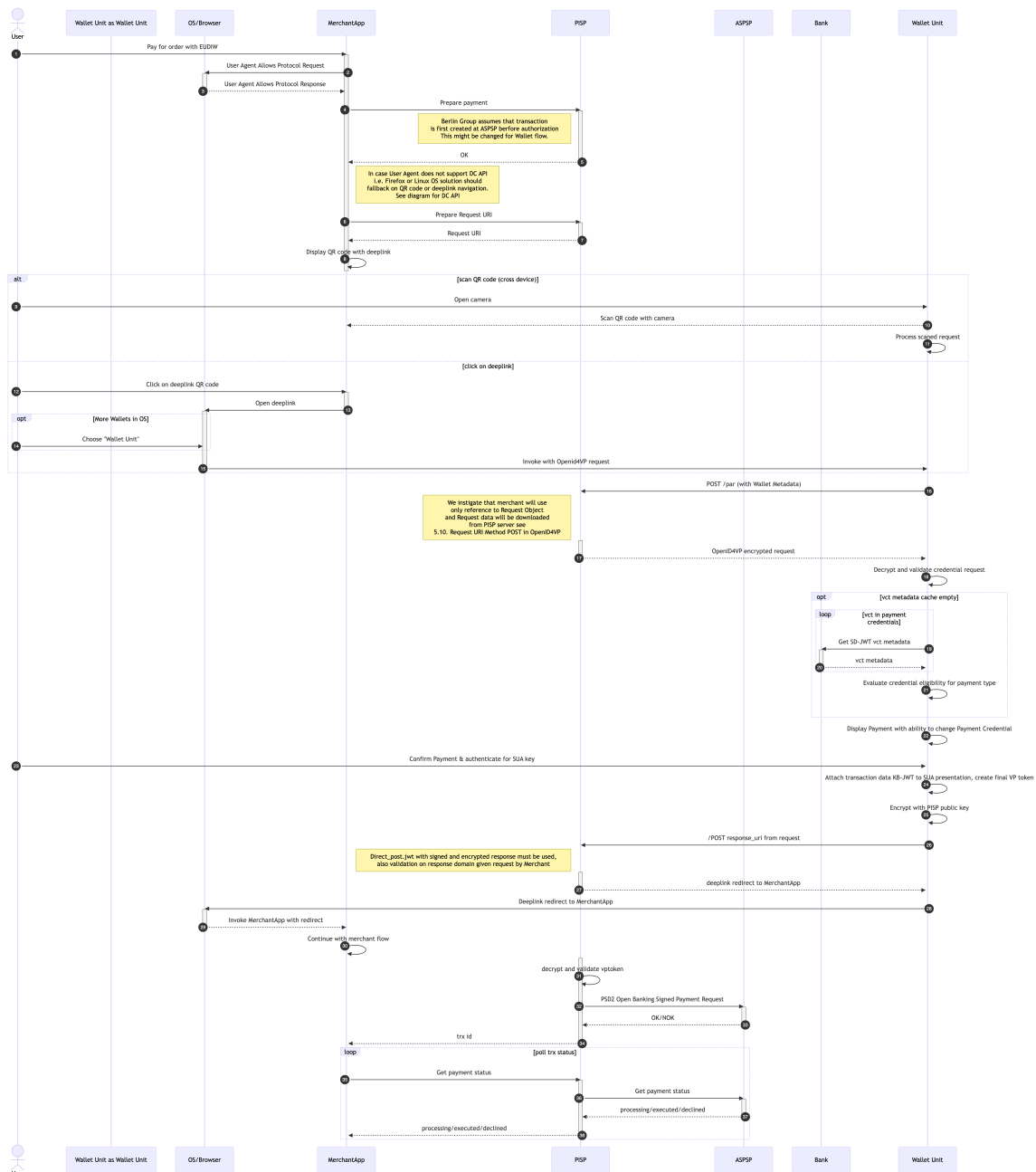
Annex 2 – Technical diagrams and examples

All technical diagrams are stored on WE BUILD GitHub <https://github.com/webuild-consortium/wp3-technology-standards/tree/main/sequence-diagrams/PA2>

DC API flow



Deep-Link API flow (same device and cross device)



Technical request examples

Details are stored on [GitHub](https://github.com/webuild-consortium/wp3-technology-standards/tree/main/examples/api-calls/PA2/A.2%20A2A%20Payment%20Initiation) <https://github.com/webuild-consortium/wp3-technology-standards/tree/main/examples/api-calls/PA2/A.2%20A2A%20Payment%20Initiation>

Signed Transaction Request spec is here: <https://github.com/webuild-consortium/wp3-technology-standards/blob/main/docs/PA2/A.2%20A2A%20Payment%20Initiation/SPR.md>

WE BUILD consortium

MVP Specifications Scenario B1 – Card- based online payment SCA with EUDIW

WP3 – UC PA2 Consumer Payments

Date : 19/6/2026
Version : 1.0
Status : For Review
Author(s) : Visa
Contributor(s): Aricoma, Authologic, Entersekt, Mastercard, Netflix, Paypal

Index

1	Introduction	4
1.1	<i>Objectives of this document.....</i>	4
1.2	<i>Scenario introduction.....</i>	4
2	Scenario specification.....	6
2.1	<i>Introduction</i>	6
2.2	<i>Scenario flows</i>	8
2.2.1	<i>Flow 1: Registration for online SCA.....</i>	8
2.2.2	<i>Flow 2: Payment / Issuer-requested SCA.....</i>	13
2.3	<i>Challenges and barriers</i>	18
2.4	<i>Working Assumptions</i>	19
3	Roles and participants	19
3.1	<i>Roles represented in the scenario.....</i>	19
3.2	<i>Scenario roles and participants.....</i>	20
3.3	<i>Additional roles and partners</i>	21
3.4	<i>Target country combinations.....</i>	21
3.5	<i>Requirements.....</i>	22
4	Attestations	23
4.1	<i>Introduction</i>	23
4.2	<i>Attestations to be provided by other UCs/WGs/scenarios</i>	23
4.3	<i>Created attestations in the scenario.....</i>	23
	Annex 1 – Requirements for scenario roles.....	25
	Annex 2 – Full list of flows as defined in the stock taking phase.....	26
	Annex 3 – Sequence diagrams	29

1 Introduction

1.1 Objectives of this document

This document describes the details of MVP scenario B1, as part of use case PA2 in work package 3 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.

A separate MVP+ specification document expands the scope with additional features and requirements.

Note: detailed technical specifications e.g sequence diagrams are available in Annex 3 and for the most up to date version on WE BUILD GitHub <https://github.com/webuild-consortium/wp3-technology-standards/tree/main/PA2> (private access, invites only)

1.2 Scenario introduction

This scenario covers how the EUDIW can be used to authenticate online card payments (often called “Pay by card”). It is part of a wider set of scenarios that have been developed in PA2:

- A1 Account-based online payment SCA with the EUDIW
- A2 Account-based payment initiation with the EUDIW
- B1 Card-based online payment SCA with the EUDIW
- B2 Card-based payment initiation with the EUDIW

The scenario is based on the following documentation:

Technology / Specification	Publication URL
ARF v2.8	https://eudi.dev/2.8.0/architecture-and-reference-framework-main/#1-introduction
ARF v2.8 Technical Specification 12	https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts12-electronic-payments-SCA-implementation-with-wallet.md
EMVco Digital Payment Credential	WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-

Draft 1.0 (19th Jan 2026)	consumer-payments/files?mid=7934&fid%5B0%5D=201&fid%5B1%5D=215&fid%5B2%5D=1232
W3C Digital Credentials API	https://www.w3.org/TR/digital-credentials/
PSD2 (Directive (EU) 2015/2366)	https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
eIDAS2 Regulation on SCA (Recital 62 and Article 5f2)	https://eur-lex.europa.eu/eli/reg/2024/1183/oj
WE BUILD WP3 PA2 Stock Taking 1.01	WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=5920&fid%5B0%5D=201&fid%5B1%5D=202&fid%5B2%5D=4208
EWC Implementation Guide 1.2	WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=866&fid%5B0%5D=201&fid%5B1%5D=202
SD-JWT VC (IETF draft)	https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/
OID4VCI 1.0	https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
OID4VP 1.0	https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
W3C Verifiable Credentials Data Model	https://www.w3.org/TR/vc-data-model/

2 Scenario specification

2.1 Introduction

To ensure compliance with eIDAS2 requirements, EU banks would have to propose the EUDIW as an alternative SCA (Strong Customer Authentication) method for online payments by the end of 2027.

SCA Attestation, Issuer-requested and 3rd party-requested flows key concepts have been designed by the previous LSPs and are defined in the ARF TS12.

This scenario, covering how the EUDIW can be used to authenticate online card payments, will include the following key features:

- registration of the citizen's EUDIW with the bank, which consist for the bank in issuing an SCA attestation. This is a pre-requisite to being able to use it as an alternative authentication method
- use of the EUDIW for SCA at an online merchant "pay by card" checkout, instead of using the legacy bank SCA method (often a bank app), based on an issuer-requested flow implementation (the bank interacts with the wallet at authentication step)
- registration and payment flows developed for same-device and cross-devices flows, using W3C Digital Credential APIs standard (depending on OEM devices support) and native OpenID4VP/VCI variants. **Not all combinations may be developed / piloted – will depend on partners capabilities**
- SCA Attestation: during the specification phase, 2 types of attestations have been designed by the WP3 T&S group for the purpose of SCA: one at card-level ("SCA-card" aka DPC or Digital Payment Credential) that leverages the EMVco DPC draft specification, and one at user-level attestation ("SCA-User" aka "Bank Key"). **The ambition is to pilot both attestations (separately or maybe with both attestations coexisting in the wallet) and evaluate the pros and cons from a business and Consumer perspective.**
- Implementation may leverage Intermediaries and/or (Q)TSPs for supporting banks and merchants' implementation in pilot

MVP flows have been listed during the Stock Taking phase and refined during the specification phase:

ID	flow name	Description	Attestations to use
1	Registration for online payments SCA	After strong authentication, registration of EUDIW instance with the bank for online payment SCA purpose, which results in the issuance of an SCA attestation. Connection to WE BUILD Trust list.	- SCA Attestation: SCA-card (DPC) and SCA-User
2	Payment / Issuer-requested SCA	Online card payment Authenticated with EUDIW previously registered with the bank. The bank (or Intermediary acting on behalf of the Bank) interacts with the wallet at authentication step. Connection to WE BUILD Trust list.	- SCA Attestation: SCA-card (DPC) and SCA-User

Note 1: network-orchestrated version of issuer-requested flows, and third-party requested flows including combined presentation are part of MVP+ specification document

Note 2: the full list of flows (MVP/MVP+) from the Stock Taking phase is listed in Appendix 2 for reference

2.2 Scenario flows

Each of the MVP flows are detailed hereafter:

2.2.1 Flow 1: Registration of the EUDI Wallet for online SCA

2.2.1.1 Main flow description

From the mobile bank portal (mobile app or website), Consumers are provided with the option to activate EUDIW to authenticate online card payments. After SCA is performed leveraging existing PSD2-compliant solution, SCA Attestation is issued to the wallet.

Supported environment:

- DC APIs and same-device flows
- SCA attestation:
 - o card-level attestation (aka DPC)
 - o user-level attestation (aka “Bank Key”)

2.2.1.2 Additional flows

The following variations and exceptions may be supported in the pilot, depending on partners capability:

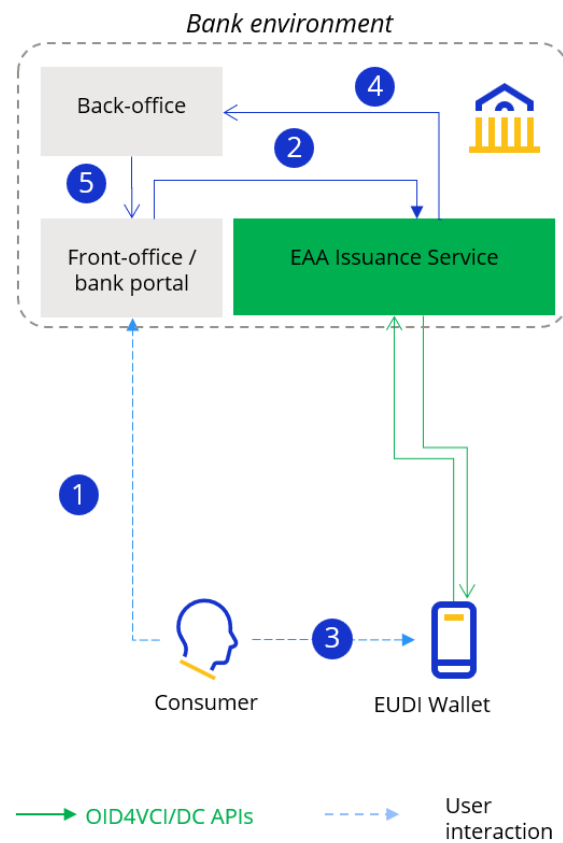
Flow	Short description
Variations	
- Cross device	QR code-based issuance of the SCA attestation
- PID verification	Optionally, depending on bank’s risk profile, verification of the PID prior to issuing the SCA attestation
Exceptions	
- Custom URI scheme fallback	If DC APIs are not available, Consumer can continue with Custom URI scheme / OID4VCI
- Other issuance channel	If bank portal/app cannot be upgraded to issue the SCA Attestation due to capacity limitations / prioritization, other issuance channels may be considered instead (e.g. manual process, call center, card network ...)

2.2.1.3 Pre-conditions

For the main flow:

- Consumer must have card(s) with the bank, and an access to the bank portal or app on mobile
- Consumer has a valid and active EUDIW, provided by either a Member State (same country than the bank) or by a private wallet provider (any country)
- Bank has updated their online banking portal / app to support the issuance of SCA attestation
- The bank (or the (Q)TSP acting on behalf of the bank) and the EUDIW must be registered in the same Trust list
- Consumer holds a mobile device compatible with DC API requirements

2.2.1.4 Flow steps



Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
1	Consumer	Consumer securely logs into online banking portal from his mobile phone and want to link his card(s) with his EUDIW for SCA. Consumer reviews T&Cs and agrees to proceed with registration		Consumer is offered to register EUDIW for SCA for online payments, login and sensitive transactions (User level SCA attestation) ... Consumer logs in from laptop
2	Bank /EUDIW/Consumer	Bank (or (Q)TSP on behalf of the bank) invokes EUDIW leveraging DC APIs and issues the SCA attestation(s) in Consumer's EUDIW	SCA Attestation based on SCA-DPC or SCA-User	Additional SCA and PID verification may apply after Consumers agree with T&Cs (depending on bank's risk appetite) If DC APIs not available, fallback to Custom URI Scheme
3	Consumer	Consumer reviews in the wallet and authenticates to accept the credential		

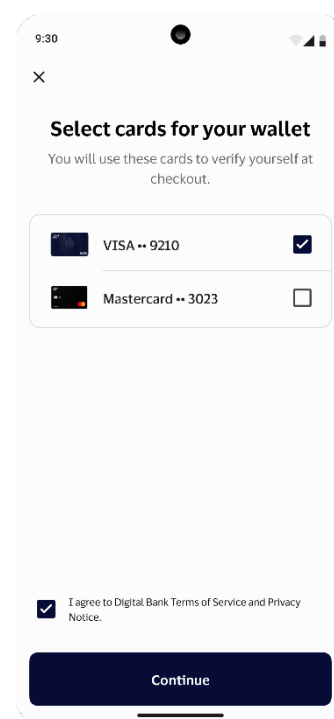
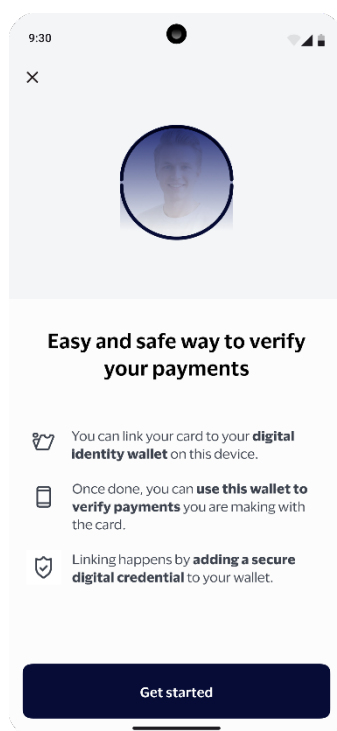
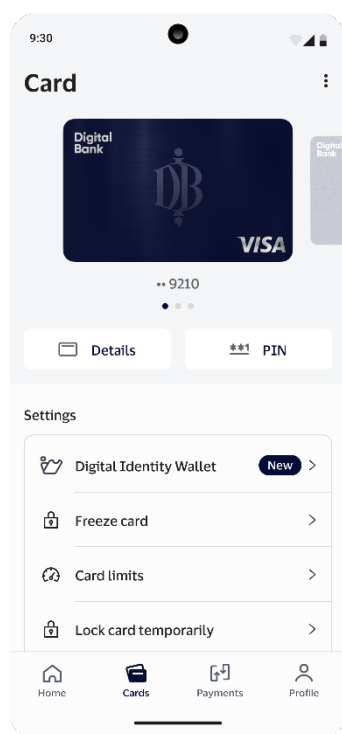
4	Bank	SCA attestation is stored in back-office, linked to the card and/or Consumer and made accessible to the authentication platforms eg ACS		
5	Bank	Bank informs the Consumer that registration is complete		

Post conditions: The Consumer can view the SCA attestation in the EUDIW

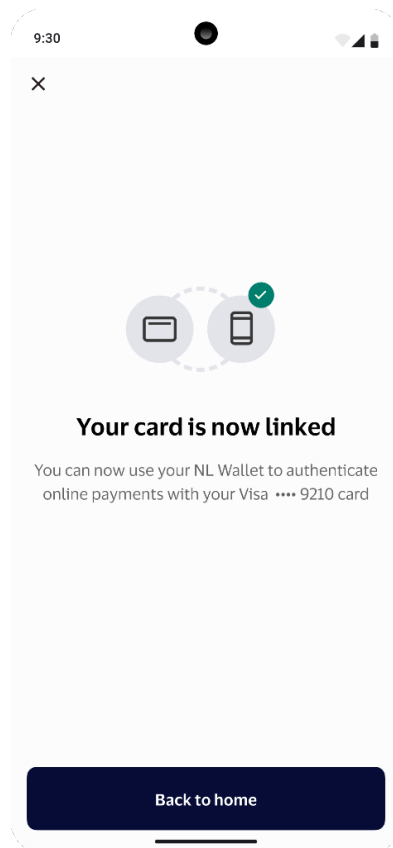
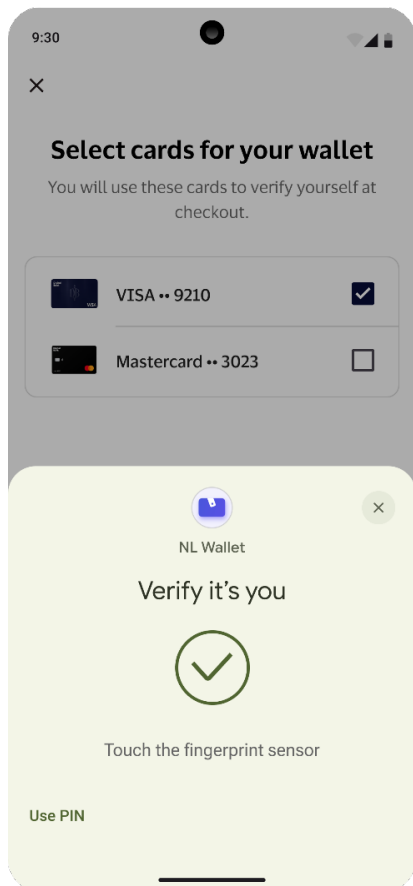
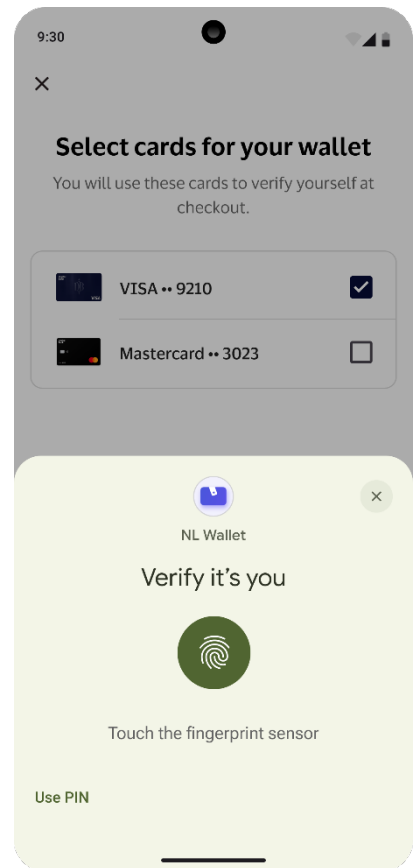
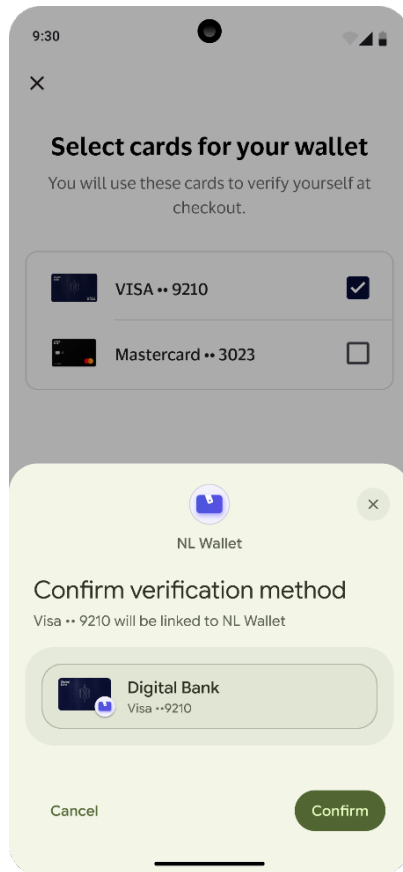
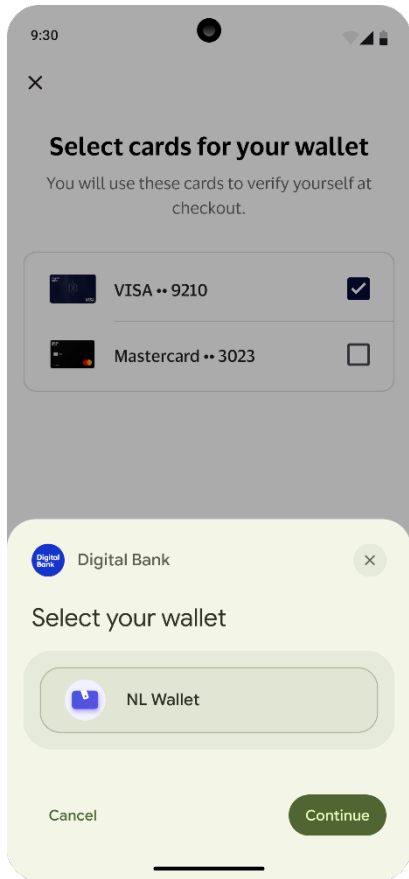
Note: lifecycle management of the attestation is not in pilot scope (either by the Consumer e.g. delete DPC from the wallet or by the bank e.g. suspend DPC for that Consumer)

2.2.1.5 UX/UI

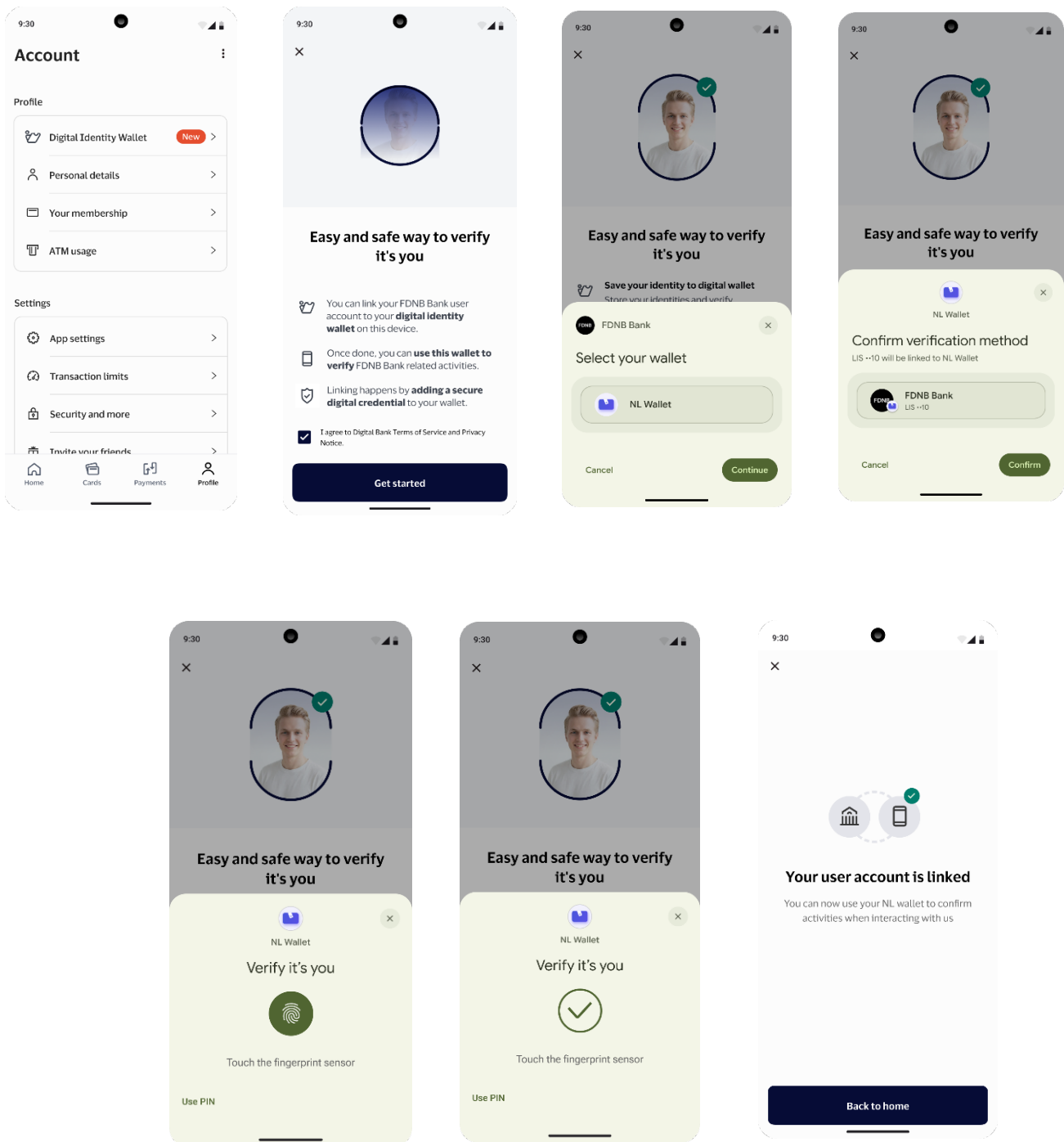
Main flow (same device/DC APIs/Card-level SCA attestation a.k.a DPC)



Note: an additional SCA step may be required by the bank after Consumer taps "continue"



Flow variant (same device/DC APIs/User-level attestation)



2.2.2 Flow 2: Payment / Issuer-requested SCA

2.2.2.1 Main flow description

The Bank (or Intermediary on behalf of the bank) interacts with the Consumer's EUDI wallet through DC APIs when performing SCA for online card payments.

Supported environment:

- DC APIs and same-device flows
- SCA attestation:
 - o card-level attestation (aka DPC)
 - o user-level attestation (aka "Bank Key")

2.2.2.2 Additional flows

The following variations and exceptions may be supported in the pilot, depending on partner's capability

Flow	Short description
Variations	
- Cross device	QR code-based interaction between the bank (or Intermediary acting on behalf of the Bank) and the EUDIW
Exceptions	
- DC API fallback	If DC APIs not available, Consumers can continue with Custom URI scheme
- Invalid SCA Attestation or EUDIW	Verification of SCA attestation fails, Bank decides to fall back to the legacy authentication method (e.g. bank app)
- Other verification channel	If bank ACS cannot be upgraded to verify the SCA Attestation due to capacity limitations / prioritization, other verification channels may be considered instead (e.g. by Card network)

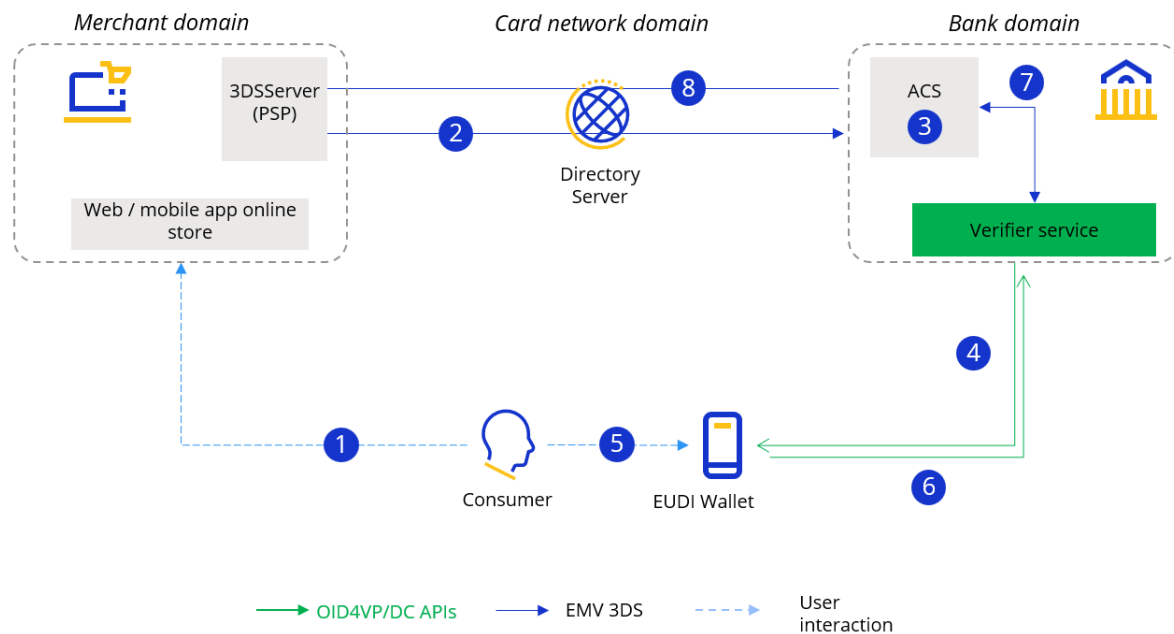
2.2.2.3 Pre-conditions

For the main flow:

- Consumer has registered the EUDIW with the bank for SCA
- Bank can detect that the Consumer has a valid SCA-enabled EUDIW and implemented a verifier capability (internally or via an Intermediary acting on behalf of the Bank)
- Bank (or Intermediary acting on behalf of the Bank) and the EUDIW must be registered in the same Trust list
- Consumer holds a mobile device compatible with DC API requirements
- Simple one-off payment (complex payments like recurring payments or instalments are not supported and will be included in MVP+ specifications)

Note: no changes are needed on the Merchant platforms for this flow for redirect-based payment page integration (changes may be needed for iFrame based integration)

2.2.2.4 Flow steps

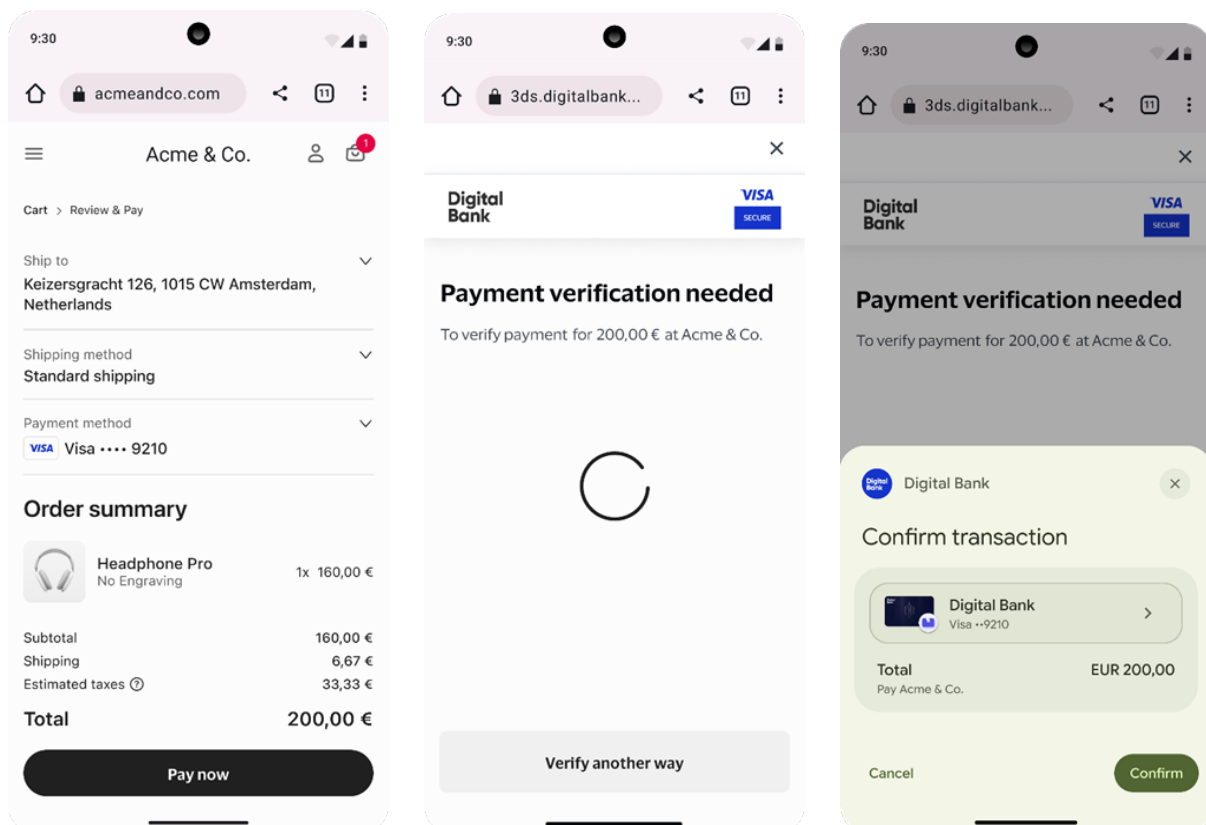


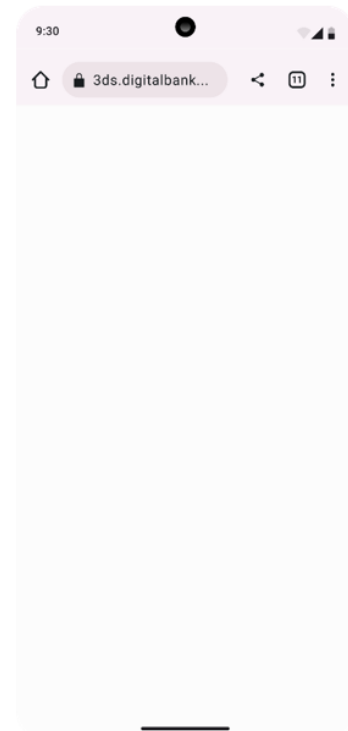
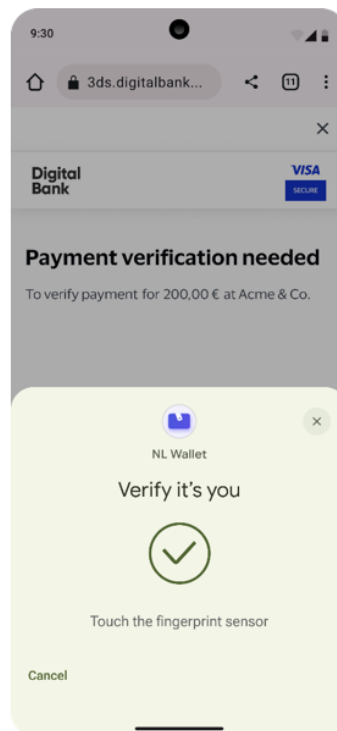
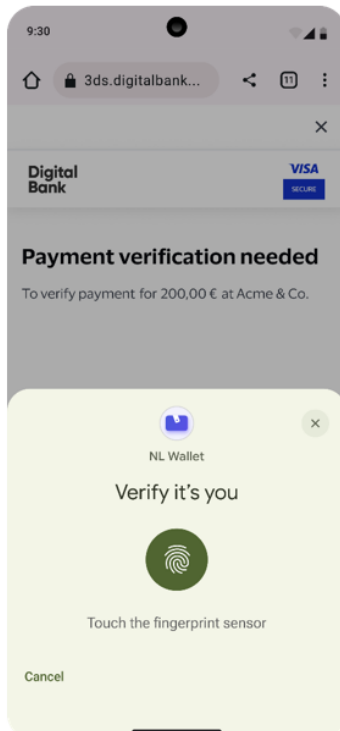
Main flow step	Actor	Interpretation or reference	Dependencies	Variations and exceptions
1	Consumer	Consumer shops at merchant from his mobile phone, proceeds to checkout chooses “pay by card” and types in card details		No manual entry needed, the card is already stored; e.g. CTP (Click-to-Pay) or merchant COF (Credential On File)
2	Merchant	Merchant (or merchant’s PSP) initiates 3DS authentication through Card network		
3	Bank	ACS recognizes that an EUDIW is linked to that PAN/Token		
4	Bank	Bank invokes wallet through verifier service		Bank may choose to provide choice of authentication method (eg 1=bank app 2=EUDIW) instead of going directly to EUDIW
5	Consumer	Consumer verifies amount and merchant name and authenticates using the EUDIW		Consumer declines the transaction and is redirected to the merchant checkout
6	EUDIW Instance	Wallet sends SCA Attestation together with Dynamic Linking evidence		
7	Bank	Bank verifies wallet output		Verification of SCA attestation fails, Bank decides to fall back to the legacy authentication method (eg bank app)

8	Merchant	Merchant receives network cryptogram from the bank and can proceed to authorization If ok, Merchant confirms to the Consumer that the transaction is complete		

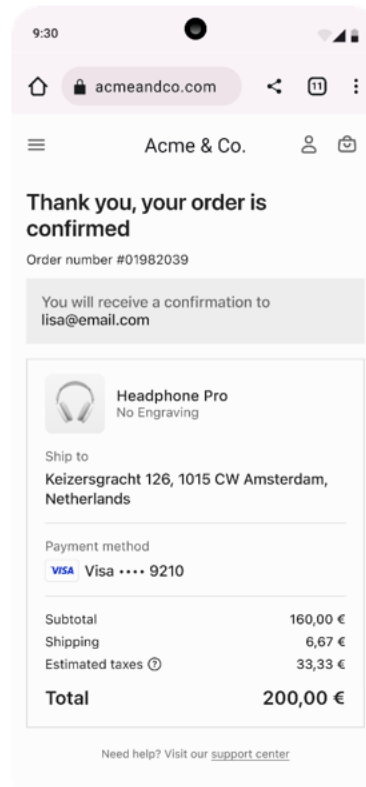
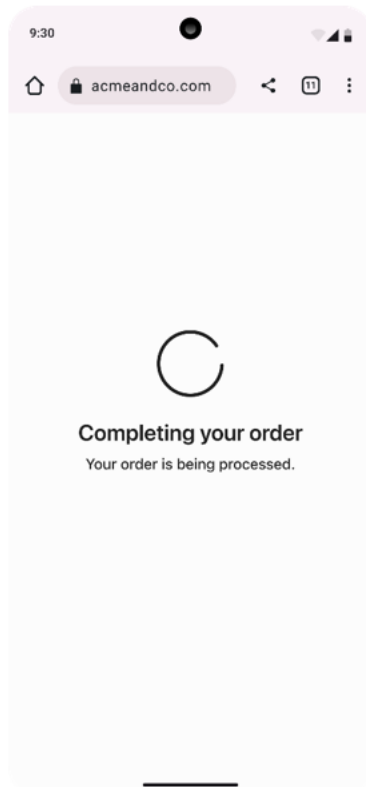
2.2.2.5 UX/UI examples

Main flow (same device/DC APIs/Card-level attestation a.k.a DPC)



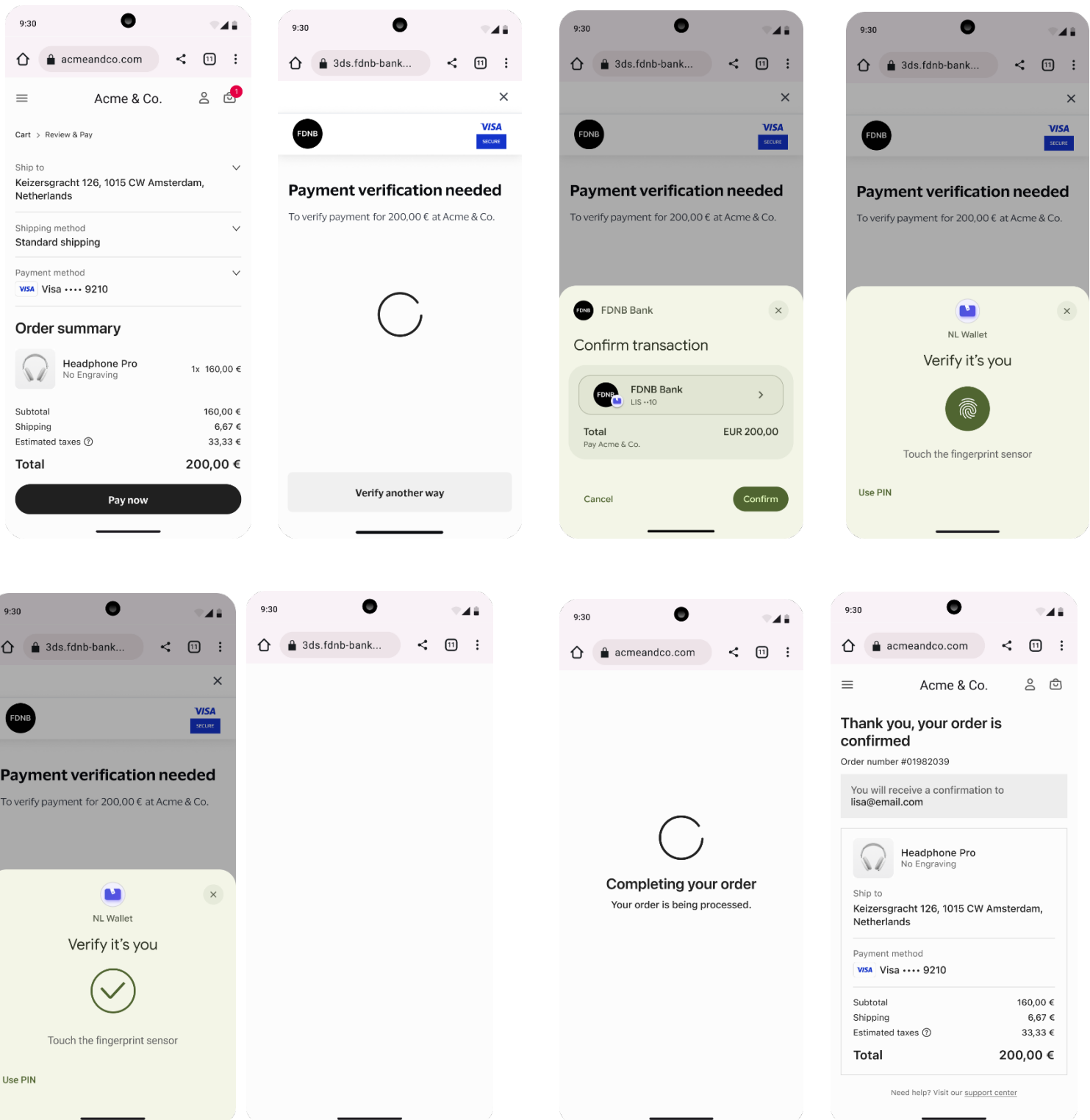


Note: Wallet may be required to display other informations at that step to comply with regulation (eg RP/Intermediary)



Note the assumption here is that, when using DC APIs, no authentication is required prior to displaying the transaction confirmation screen (with merchant name and amount), as this screen is rendered by the Platform (Credential Manager) not the Wallet (Credential Provider). In non-DC APIs flows, two authentications would be required because the confirmation screen sits within the Wallet and the ARF mandates authentication before opening it.

Main flow variant (same device/DC APIs/User-level attestation)



2.3 Challenges and barriers

Lack of maturity of available standards

- 1) **The Digital Identity/VCs standards are not mature to support payment:** we are leveraging the recently published **ARF TS12 Annex** and emerging **W3C DC APIs**
- 2) **The payment/card standards are not mature to support Digital Identity/VCs:** we will develop non-standard implementation of EMV 3DS, EMV SRC and EMV DPC for the pilot

Attestations model ambiguity

The pilot will leverage two types of SCA Attestations: a **Card-level SCA Attestation** (a.k.a DPC Digital Payment Credential), derived from EMVco DPC Draft 1.0, and a **User-level SCA Attestation** (a.k.a Bank Key) that we have defined in WE BUILD. There is uncertainty about how both should interplay together (or not), and about who should oversee and maintain the “Bank Key” in real life post-pilot.

Alignment with card standards and technologies

The solution developed in this specification document has major impacts on card standards related to payment processing, tokenization and authentication (mainly **EMV 3DS** and **EMV SRC**). If we want to build scalable solution beyond the pilot, we need to ensure strong alignment with the main standardization bodies (EMVco, FIDO Alliance)

Complexity of production banking & payment ecosystems

Uncertainty at that stage that payment partners can implement the full specifications may consequently require to reduce or adapt the pilot scope. For example, bank portal adaptation for DPC issuance is hard work; other issuance methods may be explored e.g from customer call center

Alignment with APTITUDE and the EC on TS12

Regulatory concerns from banks and governments about TS12 have emerged and have led Aptitude to pause their work on SCA and WE BUILD to collect Financial Services feedback. Dialogue between DG CONNECT / FISMA and respectively APTITUDE and WE BUILD has intensified, and as consequence, the EC is about to start regulatory and technical workgroups jointly with WE BUILD and APTITUDE. At the time of writing this document, we don't have visibility on timelines. It is highly probable that the outcome from those workgroups will impact TS12 and therefore our specifications and pilots that are based on it.

2.4 Working Assumptions

Regulatory framework

Despite recent clarifications, particularly in the European Commission FAQ, many questions remain unresolved, especially regarding liability. During that controlled pilot, we are working under the assumptions that

- SUA (Strong User Authentication) = SCA (Strong Consumer Authentication)
- banks have an obligation to accept the EUDI Wallet for online card SCA
- no outsourcing agreements are required between banks and wallets
- liability remains with the bank

Prioritized UX flow based on same device and through W3C DC API

The same-device web checkout flow will target the W3C Digital Credential API as the primary invocation mechanism, with Custom URI/native OpenID4VP as a fallback where DC API is not supported. Browser and OS support is assumed to be sufficiently available in the pilot timeframe.

The rationale for prioritizing DC APIS & same device is that 1) eCommerce is shifting/has shifted to mobile already and 2) for payment authentication flows, the UX is paramount and early research shows that the DC API UX has the potential to be superior to existing authentication methods for same device flows.

Trust services

For the pilot, issuance of the SCA attestation does not require to be Qualified: SCA Attestations are EEAs issued by TSPs (as opposed to QEAs issued by QTSPs)

Pre-production environment

The pilot aims to experiment with real payment transactions at real merchants based on real cards issued by real banks in a controlled environment (eg limited SLAs, restricted access to project team and/or friends&family, ...)

Pilot KPIs (number of transactions, etc ...) will be defined with the pilot partners

3 Roles and participants

3.1 Roles represented in the scenario

- Authentic Source / Issuer of SCA Attestation:
 - Bank 1 – Country A
- Relying Parties:
 - Bank 1 – Country A (bank act as both Issuer and Verifier of the SCA attestation)
- Holder 1
 - Country A Natural Person – existing client of Bank 1
- Wallet Provider 1 – Country A

- Authentic source / Issuer of PID Attestation:
 - Member State/PID provider for Country A
 - or derived PID by private wallet

In addition of eIDAS2 roles above, key technology partners would also need to support the scenario:

- Bank 1 partners:
 - Online/mobile banking infrastructure provider (if online/mobile banking is not done in-house)
 - ACS provider (if not developed in-house)
 - Card network (Directory Server)
 - Authentication platform technology provider (if not developed in-house)
 - Intermediary (if not developed in-house)
 - EEA issuer (of the SCA Attestation)

Note:

- Consumer citizenship is determined by the bank country
- Because this MVP is focusing on issuer-requested flows, only the banks are interacting with the wallet and are therefore the Relying Parties.
- Merchants should not be technically impacted and are not per se Relying Parties but can still participate in a pilot by e.g. providing test accounts, enabling refunds after a successful authenticated payment, monitor checkout performance, etc ...

3.2 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of EUDI Wallet	Banca Transilvania Consumer	RO
	Sparebank 1 Consumer	NO
	Caixabank Consumer	SP
2. Authentic sources	Banca Transilvania	RO
	Sparebank 1	NO
	Caixabank	SP
3. Relying party	Banca Transilvania	RO
	Sparebank 1	NO
	Caixabank	SP
4. Intermediary	Veridas (for Caixabank)	
	Visa (for Banca Transilvania and Sparebank1)	
	Other partners that may provide additional service to existing banks or bring additional banks to pilot: Authologic, Hopae, iGrant.io, Lissi, Netcetera, Mastercard, Paypal, Worldline	

3.3 Additional roles and partners

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	Google Wallet	RO (tbc)	NW
	GRNET	GR	NW
	iGrant.io	NO	NW
	Veridas	SP	NW
2. PID Provider	GRNET	GR	NW
3. Trusted list registrar	n/a		NW
4. QEAA provider	n/a (assumption that this scenario attestations do not require Qualified services)		NW
5. Pub-EAA provider	n/a		NW
6. EAA provider	Veridas (for Caixabank)	SP	NW
	Visa (for Banca Transilvania and Sparebank1)	EU	NW
	Other partners that may provide additional service to existing banks or bring additional banks to pilot: Authologic, iGrant.io, Lissi, Netcetera, Mastercard, Worldline		NW
7. QES provider	n/a		NW
8. Bank payment partners (ACS, Open Banking APIs, ...)	BPC, Entersekt, Netcetera, Worldline ACS		NW
9. Card Schemes	Mastercard, Visa		NW
10. Merchant payment partners (PISP, PSP/Acq, 3DS Server, ...)	Adyen, Netcetera, PayPal, Worldline		NW
11. Merchants	Netflix	n/a	NW
	Cyclades Fast Ferries	GR	
	Other partners that may provide support: Google Store, Adyen		
12. Other partners	University of the Aegean, Obserwatorium.biz		NW

3.4 Target country combinations

This MVP is focusing on issuer-requested flows, the banks are both Issuers and Relying Parties. Cross border combination is determined by:

- Issuing country = Bank and Consumer country
- RP country = Merchant country

	Issuing country						
Relying Party country		RO	NO	SP			
	GR	Y	Y	Y			
	EU (*)	Y	Y	Y			

(*) exact countries of Netflix.com tbd, but the plan is to test from 3 countries

3.5 Requirements

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

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 credential containing core identity attributes of a natural person, such as: • Given name / family name • Date of birth • Unique personal identifier • Nationality PID is issued by a PID provider (typically a member state authority/ member state designated authority)	WP4	GR	PID to be issued in the EU-DIW to make it a 'Valid' EU-DIW instance. PID may be required by the bank when registering the EUDIW
Derived PID	Alternatively, a PID could be derived from a passport and issued by a private wallet after Consumer onboarding (passport scan, liveness detection, ...)	WP4	RO, NO, SP	

4.3 Created attestations in the scenario

Attestation name	Short description	For Countries	Applicable domain standards
SCA-card v1.0	A.k.a Digital Payment Credential (DPC) and based on EMVco DPC Draft 1.0 The DPC is a structured, selectively disclosable representation of a digitized payment card This attestation is used for online card payment SCA purpose.	RO, NO	EMVCo
SCA-user v1.0	A.k.a as "Bank Key" SCA User attestation specify User level SUA attestation described in TS12 published by European Commission. SCA	SP	

	User attestation represents User that is using EUDI Wallet for authentication and risk operation authorisation in theirs online banking, banking mobile application, 3DS flows and similar		
--	--	--	--

Annex 1 – Requirements for scenario roles

This annex lists the main functional/organizational/technical requirements for each role in the scenario. This will be refined in the pilot project phase.

Primary role	Specific requirement
1. User of EUDI Wallet	a. Must be a bank Consumer and has a card
	b. Should be a citizen of the same country that his bank
	c. Should have a mobile device compatible with DC API
2. Authentic sources	a. (banks) Should implement SCA Attestation issuance from bank portal
	b. (banks) Must adapt their ACS and Authorization platforms to support EUDIW based SCA
3. Merchants	a. Should monitor checkout performance
	b. Should provide test accounts
	c. Must implement refunds capabilities
4. Intermediary	a. Must provide APIS to banks to verify SCA Attestations
	b. Must support DC APIs
5. EUDI Wallet provider	a. Must implement ARF TS12
	b. Must support DC APIs
	c. Must implement UX/UI as defined in that document
	d. Could issue a derived ID (e.g. based on passport) if no PID provider available
6. PID Provider	a. Should Provide PID
7. Trusted list registrar	a. Must register banks and/or their intermediaries in WE BUILD Trust list
	b. Must register wallets in WE BUILD Trust list
8. QEAA provider	a. N/A
	b. N/A
	c. N/A
9. Pub-EAA provider	a. N/A
	b. N/A
	c. N/A
10. EAA provider	a. Must provides APIs to banks to issue DPC and Bank Key attestations
11. QES provider	a. N/A
	b. N/A
	c. N/A

Annex 2 – Full list of flows as defined in the stock taking phase

High level flows from the Stock Taking phase

The stock taking phase has confirmed the following scope for the B1 pilot scenario:

ID	Scenario name	Flows Description	Attestations to use	Proximity or Remote	MVP
B1	Card online SCA	Issuance of SCA attestation from bank portal (idem A1) – use of EUDIW for card online SCA both Issuer-requested SCA Or Third-party-requested SCA with combined presentation and W3C DC APIs - Connection to WE BUILD Trust infrastructure	- SCA Attestation - PID for age	Remote	Y
B1 +	Advanced Card online SCA	B1 + one or many of: SCA Attestation lifecycle management; Merchant integration options; PSP/Acquirer-captured SCA; issuance of SCA attestation from EUDIW; issuance of merchant attestation; ID check at parcel collection; recurring payment; merchant provides proof of ID to bank;	Same as above Depending on partners, other attestations may be used (eg Student, Loyalty, eReceipt, ...)	Remote / Proximity	N

Detailed Flows

ID	flow name	Description	Attestations to use	Proximity or Remote	MVP
1	Bank portal / Registration for online payments	From secure online banking environment and after strong authentication, registration of EUDIW instance with the bank for online payment SCA purpose / Issuance of SCA attestation	- SCA Attestation	Remote	Y
1b	Bank portal / SCA attestation LCM	Lifecycle management (revocation, suspension, ...) of SCA attestation	- SCA Attestation	Remote	N
1c	Bank portal / registration	Optional additional control using the PID at registration	- SCA Attestation - PID (optional for registration)	Remote	N

	n with PID				
2	Payment / Issuer-requested SCA	Online card payment Authenticated with EUDIW previously registered with the bank. The bank interacts with the wallet at authentication step (formerly “bank-led SCA” flow). Connection to WE BUILD Trust list.	- SCA Attestation	Remote	Y
2 b	Payment / Combined Issuer-requested SCA	Same as above + combined presentation with age 18+ Confirmation of age sent back to the merchant by the bank over EMV 3DS rails	- SCA Attestation - PID for age	Remote	N
3	Payment / Third-party-requested SCA	Online card payment Authenticated with EUDIW previously registered with the bank. The merchant interacts with the wallet, captures the authentication data and send it back to the bank over EMV 3DS rails (formerly “merchant-captured” flow). Connection to WE BUILD Trust list.	- SCA Attestation	Remote	Y
3 b	Payment / Combined Third-party-requested SCA	Online card payment Authenticated with EUDIW by the merchant with combined presentation of age 18+ (see 2b)	- SCA Attestation - PID for age	Remote	Y
3 c	Payment / Combined Third-party-requested SCA with attestation issuance	Same as above + merchant to issue attestations when payment approved	- same as 3b - eReceipt, ticket, boarding pass, ... depend on pilot partners	Remote	N
4	Payment / Merchant integration options	For workflows 2 & 3, consider technical integration options: redirect, iFrame, inApp, COF/CtP, ...	- same as 2 & 3	Remote	N
5	Payment / PSP/Acquirer captured SCA	The PSP/Acquirer is the Relying Party capturing the SCA on behalf of the merchant	- same as 2 & 3	Remote	N
6	ID Check on delivery	Use of EUDIW to check the ID of the recipient of goods in face to face (delivery fraud)	Tbd	Proximity	N
7	ID Verification with guest checkout	Consumer has Digital ID but not Digital Payment credential in wallet. Merchant provides proof of ID /age and name. Issuer verifies that ID	PID	Remote	N

		matches payment information provided			
8	Signing a mandate using the SCA attestation	Collect consent for recurring payment such as a subscription to a streaming service, the EUDIW generates a verifiable credential that cryptographically binds the subscription confirmation (merchant, start date, duration contact and selected card id) using the SCA attestation. Independently of the way the payment instrument (card, IBAN) has been provided to the merchant (could have been provided by the EUDIW, or manually typed in by the Consumer) Management of user mandate (amount, revoke, suspend, ...) in the wallet	Digital Payment Credential (Payment Attestation) – capturing subscription confirmation	Remote	N

Annex 3 – Sequence diagrams

The source and most up to date versions can be found on WE BUILD GitHub

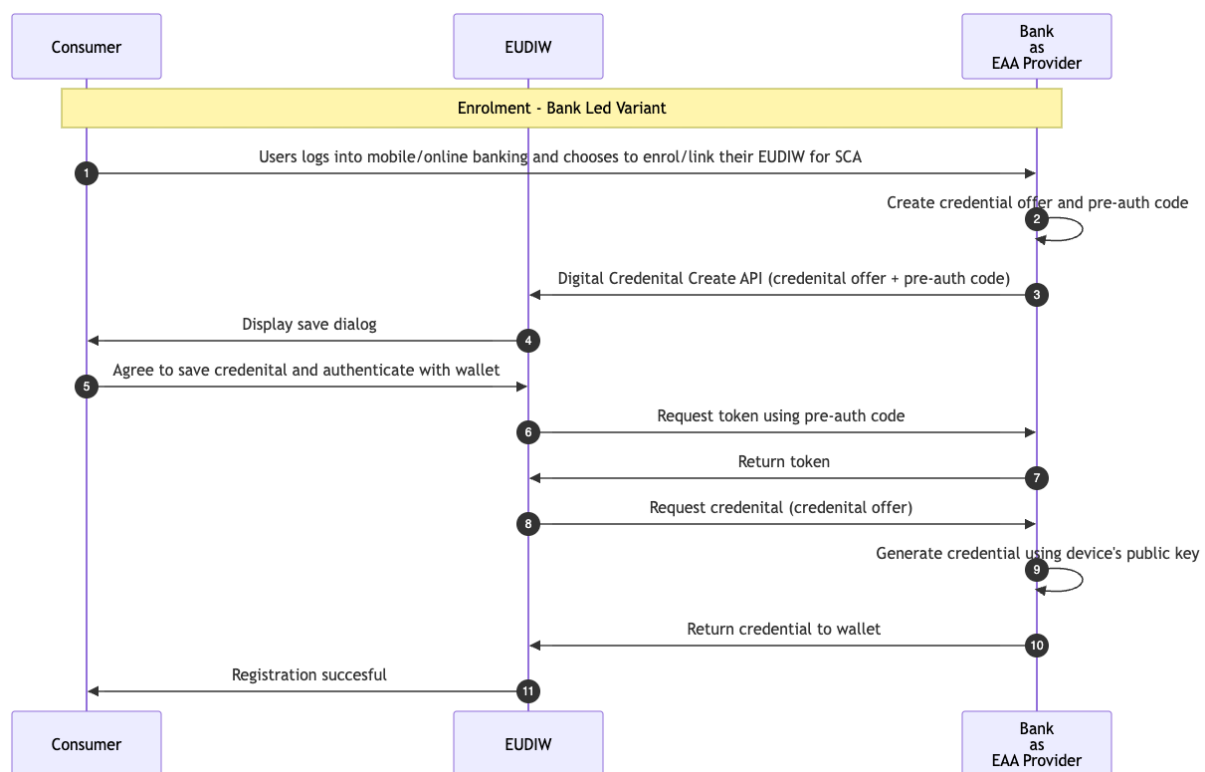
<https://github.com/webuild-consortium/wp3-technology-standards/tree/main/sequence-diagrams/PA2/B.1%20Cards%20SCA>

Assumption is that the flows hereafter are valid for same and cross device flows, using DC APIs or Custom URI Scheme (OID4VCI/VP). Detailed sequence diagrams that describe interactions with the EUDIW for payment are available here <https://github.com/webuild-consortium/wp3-technology-standards/tree/main/sequence-diagrams/common>

Note: access to this GitHub repo is private and requires approval

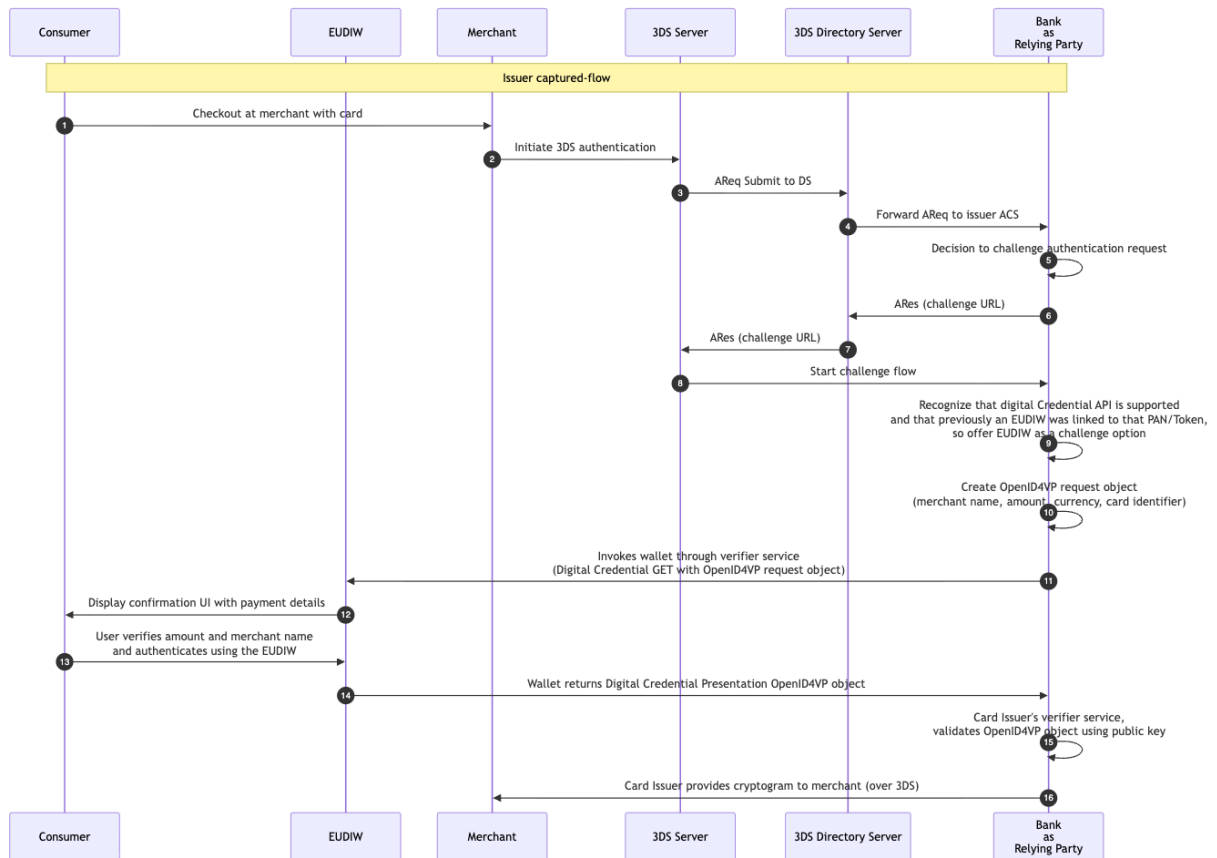
Flow 1: Registration of EUDIW for online SCA

The bank issues the SCA Attestation in the EUDI wallet.



Flow 2: Payment / Issuer-requested SCA

The bank invokes the wallet at authentication step



WE BUILD consortium

MVP Specifications

Scenario B2 - Card-based payment initiation with EUDIW

WP3-PA2 Consumer Payments

Date : 19/06/2026

Version : 1.0

Status : For review

Author(s) : Mastercard

Contributor(s) : OP bank, G+D Netcetera, Aricoma, Lissi, iGrant, Cyclades Fast Ferries, University of Aegean

Contents

1	Introduction.....	3
1.1	Objectives of this document	3
1.2	Scenario introduction	3
1.2.1	Attestations to be used	4
1.2.2	Payment Terminology.....	5
2	Scenario Specification	5
2.1	Introduction.....	5
2.2	Scenario Flows.....	7
2.2.1	MVP Flow 1: Provisioning of DPC through EUDIW	7
2.2.2	MVP Flow 2: Presentation of DPC- Payment Initiation (Guest Checkout) using EUDIW	15
2.2.3	MVP Flow 3: Presentation of DPC- Payment Initiation + Combined Presentation (Enhanced Guest Checkout).....	28
2.3	EUDIW checkout experience: Integration Options.....	40
2.3.1	Integration options: Explained	41
2.4	Challenges and barriers.....	44
2.4.1	Wallet discovery and branding on merchant checkout page	44
2.4.2	W3C Digital Credential API Maturity and Support.....	44
2.4.3	DPC Schema Standardization.....	44
2.5	Working Assumptions	45
2.5.1	Standards Maturity (DPC, DC API)	45
2.5.2	W3C DC API considered as primary invocation mechanism	45
2.5.3	Trust Infrastructure availability	45
2.5.4	PID availability	45
2.5.5	Consumer identification:	46
3	Roles and participants.....	46
3.1	Roles represented in the scenario.....	46
3.2	Scenario roles and participants	47
3.3	Additional roles and partners.....	47
3.4	Target country combinations	48
4	Attestations	48
4.1	Introduction.....	48
4.2	Attestations to be provided by other UCs/WGs/scenarios	48
4.3	Created attestations in the scenario	49
	Annex 1 Requirements for scenario roles	50
	Annex 2 Sequence Diagrams	54

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario B2, as part of use case PA2 in Work Package 3 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 covers how the EU Digital Identity Wallet (EUDIW) can be used for card payment initiation a.k.a. Guest Checkout, where a customer selects 'EU Digital Identity Wallet' as a payment option on merchant's checkout environment. It is part of a wider set of scenarios that have been developed in PA2:

- A1 Account-based online payment SCA with the EUDIW
- A2 Account-based payment initiation with the EUDIW
- B1 Card-based online payment SCA with the EUDIW
- B2 Card-based payment initiation with the EUDIW

The scenario is based on the following documentation:

Technology / Specification	Publication URL
ARF v2.9	European Digital Identity Wallet - European Digital Identity
ARF Technical Specification 12	https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts12-electronic-payments-SCA-implementation-with-wallet.md
EMVco Digital Payment Credential Draft (DPC) 1.0 (19th Jan 2026)	WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=7934&fid%5B0%5D=201&fid%5B1%5D=215&fid%5B2%5D=1232
W3C Digital Credentials API	https://www.w3.org/TR/digital-credentials/
PSD2 (Directive (EU) 2015/2366)	https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng

WE BUILD WP3 PA2 Stock Taking 1.01	WE BUILD Portal https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=5920&fid%5B0%5D=201&fid%5B1%5D=202&fid%5B2%5D=4208
SD-JWT VC (IETF draft)	https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/
OID4VCI 1.0	https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
OID4VP 1.0	https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
W3C Verifiable Credentials Data Model	https://www.w3.org/TR/vc-data-model/

1.2.1 Attestations to be used

Below attestations are used in this scenario:

1. **Digital Payment Credential (DPC)** : A Digital Payment Credential is a cryptographically verifiable digital credential, bound to a payment instrument, that is issued within a defined trust framework and can be presented by a wallet to a relying party to support authentication and/or initiation of payment transactions in a secure, privacy-preserving, and interoperable manner.

DPCs are currently being standardized for card payments within EMVCo*, including the definition of their conceptual model and technical schema to ensure consistency and interoperability across the payment ecosystem.

For the purpose of this pilot, the DPC is used as a card payment attestation which contains a Card ID (instead of a card token) that references a cloud-stored payment token (e.g., SRC token), along with cryptographic proof of user authentication and cardholder intent.

*EMVCo: Global technical body managing EMV (Europay, Mastercard and Visa) specifications for secure, interoperable card-based payment transactions.

2. **‘Proof of eligibility’**: This term applies to any attestation which provides evidence of a consumer’s eligibility to purchase goods or access services across a range of use cases. For the purpose of this flow, a generic term is used to ensure flexibility and applicability across different use cases.

Such an attestation may take various forms depending on the context, including:

- A student ID, enabling access to student-specific benefits such as discounts
- A driving licence, supporting use cases such as car rental eligibility

- A derived attribute from an existing credential (e.g., an age-over-18 attribute derived from a PID credential)

1.2.2 Payment Terminology

1. **Card network tokenization system:** A payment security system that replaces sensitive card data (e.g., PAN) with a non-sensitive token, which is used to process transactions without exposing the actual card details.

For the purpose of this pilot, the card tokenization system referenced in the design is based on **Mastercard's Secure Remote Commerce (SRC) system**. While other card schemes may leverage their own scheme-specific tokenization systems, the underlying implementation models described in this specification is expected to remain largely consistent.

2. **Card Payment Authorization:** Card Payment authorization is the process by which a transaction is routed through the card network to the issuing bank for approval or decline, where the issuer validates card details, available funds or credit, and risk parameters before reserving the funds.

2 Scenario Specification

2.1 Introduction

This scenario covers the card-based payment initiation method a.k.a. Guest Checkout where a consumer selects '**EU Digital Identity Wallet**' as a payment option on merchant's e/m-commerce checkout environment. The scenario will include the following key use cases and features:

1. Provisioning of the consumer's card based Digital Payment Credentials (DPC) in their EUDIW. This will require an issuing bank or a bank designated EAA provider to issue a DPC (Digital Payment Credential) for the card of choice. This is a pre-requisite for using EUDIW for card payment initiation.
2. Guest checkout using EU Digital Identity Wallet (EUDIW) for card payments at an online merchant. Among various payment options available on the checkout page the consumer selects 'EU Digital Identity Wallet' as a payment option.
3. Enhanced guest checkout; same as above (2) combined with a presentation of 'proof of eligibility' (e.g. age claim, Student ID, Loyalty card etc.) on merchant's request.
4. Both provisioning and payment flows are developed using W3C Digital Credential APIs standard (depending on OEM devices support) and native OpenID4VP/VCI

variants. Not all combinations will be piloted the most relevant ones will be selected based on partner availability and timelines.

Below MVP flows have been listed during the Stock Taking phase and refined during the specification phase:

ID	Flows	Description	Attestations to use/issue	Proximity or Remote	MVP
1	Provisioning of DPC from EUDIW	Issuance of the card payment credential (DPC) from the EUDIW itself	Digital Payment Credential (Card Payment Attestation)	Remote	Y
2	Guest Checkout using EUDIW	Guest Checkout with EUDIW selected as a Payment option (for card payment) on same device. Payment instrument reference is returned in the form of a DPC, that also provides proof of authentication.	Digital Payment Credential (Card Payment Attestation)	Remote	Y
3	Enhanced Guest Checkout using EUDIW (Combined presentation)	Same as (2) along with 'proof of eligibility' presentation (ex: age claim, shipping address, loyalty card, student card etc.) from EUDIW delivered back to the merchant	Digital Payment Credential (Card Payment Attestation) + other attestation(s) such as the PID, Student attestation	Remote	Y

Note: Age verification is a high-priority use case on the European Commission's agenda and is therefore considered as the preferred combined presentation use case for this pilot. However, at this stage, no participating merchant in PA2 is able to support a direct age-restricted merchant use case (e.g. alcohol sales). Consequently, we are developing an alternative combined presentation use case based on student attestation/ loyalty card presentation, which can be supported by currently confirmed merchant partner: Cyclades Fast Ferries / University of the Aegean.

2.2 Scenario Flows

2.2.1 MVP Flow 1: Provisioning of DPC through EUDIW

2.2.1.1 Main flow Description

This flow describes the issuance of a Digital Payment Credential (DPC) happening through an EU Digital Identity Wallet (EUDIW) where a consumer initiates issuing of a Digital Payment Credential (DPC) into their EU Digital Identity Wallet (EUDIW) via a wallet provided option (e.g. ‘Add Credential’/ ‘Add Card’).

Once issued, the DPC can be used for secure authentication of card-based checkout transactions using EUDIW.

Supported MVP environment:

- Mobile device (Android), same device
- Attestation: Digital payment Credentials (DPC)

Pilot Operating Model:

In this flow:

1. The card network operates as an Electronic Attestation of Attributes (EAA) provider on behalf of the issuing bank, an approach adopted to minimize integration complexity for issuing banks and to align with pilot timelines. In this model, the card network leverages its tokenization system (as explained in section 1.2.2) to facilitate credential issuance.

Alternative implementation models (e.g. banks or other TSPs acting as an EAA provider etc.) are possible and can be explored outside the scope of this pilot.

2. To reduce integration complexity for EUDI Wallets and prevent one-to-one integration with multiple card schemes or issuers, a new role is introduced in this flow- **The Credential Issuance Facilitator (CIF)**, which supports DPC provisioning by orchestrating interactions between EUDI wallets and card networks. Within WE BUILD context this role will be aligned with the WP4 architecture.

In the DPC context, the CIF:

- Facilitates secure discovery and identification of card references via card Network systems (e.g. Click to Pay / SRC profile)
- Coordinates issuer-led authentication (e.g. EMV 3DS) prior to DPC issuance
- Triggers DPC issuance by the issuer or its delegated network service

- Facilitates wallet providers' integration with multiple credential issuers, including conformance and acceptance requirements.

The CIF does not issue DPCs and does not assume issuer liability.

Roles and Responsibilities (Pilot Scope):

Actor	Role/Acting as
Consumer	Holder
Bank	Card Issuer/ACS; ACS may be operated by bank or by an authorized technology provider acting on behalf of the bank.
Wallet	EU Digital Identity Wallet
Credential Issuance Facilitator	Integrates with wallet; orchestrates interaction between EUDIW and Credential issuer/EAA provider (e.g. card N/W or banks)
Card Network	EAA Provider (on behalf of bank)

2.2.1.2 Additional Flow

The following variations may be supported in the pilot

Flow	Short description
Variations	
DPC Provisioning happening via Card N/W domain or issuer domain without CIF involvement	Wallets can redirect the user to a Card N/W or issuer-controlled domain instead of a Credential Issuance Facilitator domain for DPC provisioning.
Manual card entry	Instead of selecting the card from a pre-populated list in the CIF or EAA provider domain, the consumer chooses to manually enter the card details for DPC issuance.
Exceptions	
-	-

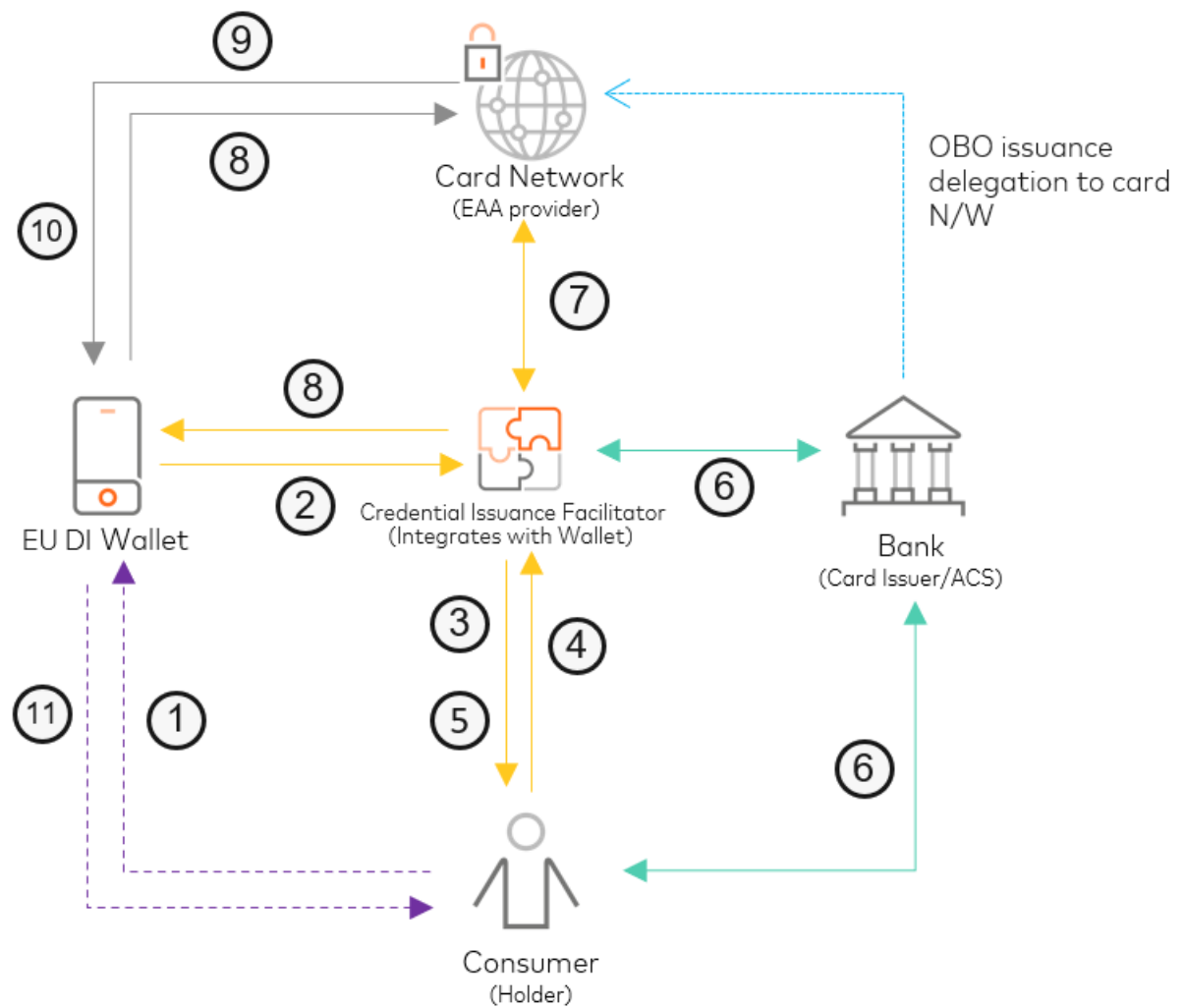
Same-Device Assumption:

As the DPC provisioning flow is initiated within the EUDI Wallet, the issuance process is expected to occur on the same device. Consequently, cross-device scenarios are out of scope for this flow.

2.2.1.3 Pre-conditions

- Consumer must have an EUDI Wallet instance from a “valid” EUDI wallet solution provider. EUDIW instance must be registered in the Trust List Provider (TLP) with ‘valid’ status.
- Consumers have completed their account registration on EUDIW application including the successful issuance of Person Identification Data (PID) in their wallet.
(Note: for this pilot PID issuance is expected to be managed by WP4 group)
- Consumers have a valid and active payment card issued by an issuer (Bank).
(Note: For this pilot, it is assumed that selected consumer shall already possess an existing payment card and will act as an EUDI Wallet holder)
- The bank, EAA provider acting OBO bank and EUDIW must have their Trust Anchors registered in the same Trust framework.
(Note: for this pilot the Trust framework will be issued and managed by the WP4 group)
- The PSP (Bank) to perform identity & verification (ID&V) process using EMV 3DS challenge authentication flow (NPA) before issuance of DPC in the EUDI Wallet.
- Bank’s existing agreement with card network tokenization system has been updated to include provisions covering the use of card network tokenization system for EUDI Wallet based card credential creation.
(Note: This update is not mandatory for pilot participation but is expected to be addressed as part of a production-ready deployment).

2.2.1.4 Flow Steps



Trigger: While authenticated in their EUDI Wallet application, the consumer (holder) initiates the issuance of digital payment credentials in order to use the wallet as a guest checkout payment method for future online transactions performed with their payment card.

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
1: Consumer access the EU Digital Identity (EUDI) Wallet for adding card credential	Consumer/ Holder	Consumer logs into the EUDI Wallet instance and proceeds to add a Digital payment Credential (DPC) for a payment card by selecting ‘ Add Credential ’ feature/button followed by ‘ Credit/debit Card ’ feature/button.	For a EUDI Wallet instance to be ‘valid’. A PID should be issued in the wallet which is expected to be provided by WE BUILD WP4 group	Variation: The wallet can also provide card scheme specific button in their interface e.g. ‘Add Mastercard/ Visa’
2: The EUDI Wallet redirects the user to a CIF/EAA provider’s domain	EUDIW	The wallet opens a secure web view (e.g. Chrome Custom Tab) redirecting the user to a credential issuance facilitator (CIF) domain acting on behalf of the EAA provider.		Variation: Based on implementation choice, EUDIW can also redirect the consumer to a card-network or bank-controlled domain,
3: Consumer/ Card identification	Credential Issuance Facilitator (CIF)	Using an existing secure identifier (e.g. verified email address/phone no.), the Credential Issuance Facilitator steps in to identify if the consumer already has card stored in card network tokenization systems.		Variation: The consumer can also select an option for a Manual card entry (e.g. PAN, expiry date)- Skip to step 5
4: Card selection by Consumer	Consumer/ Holder	The consumer selects the card to be provisioned using: Card selection from a list generated after the user is recognized by the CIF (through an existing card profile e.g. Click to Pay)		Variation: In case of manual card entry, the CIF identifies the card network.
5: Terms & condition approval by consumer	Credential Issuance Facilitator (CIF)/ Consumer	At this stage the CIF will display bank’s (card issuer) T&Cs related to the card usage in EUDIW. <i>(Note: This update is not mandatory for pilot participation but is expected to be addressed as part of a production-ready deployment).</i> The consumer accepts the T&Cs.	The consumer can choose to decline the T&Cs at this stage	Variation: T&C’s to be displayed in card or issuer-controlled domain.

6: Identity and Verification by bank	Bank (Card issuer)	Prior to adding the card to the wallet, the bank's ACS performs additional Identification & Verification (ID&V) checks. For the pilot, this is executed using a challenged bank-led authentication flow (e.g. EMV 3DS non-payment authentication).		Variation: ACS may be operated by an authorized technology provider acting on behalf of the bank.
7: Token retrieval from EAA provider	Credential Issuer Facilitator (CIF)	Upon successful authentication, the CIF connects with the EAA provider (card network) to get the Token.		Variation: CIF Can connect with Bank or another Trust service provider (TSP) acting as an EAA provider
8: Token handover to wallet for EAA interaction	EUDIW	The CIF then passes the token to the wallet using which the wallet communicates directly with the EAA provider for DPC issuance		
9: DPC issuance by EAA provider	EAA Provider	The EAA Provider (card network) issues the Digital Payment Credential (DPC). The issued DPC contains a 'Card Identifier', which references a network managed payment token or card record, along with cryptographic binding to the authenticated user and device.	DPC attestation based on SCA DPC as defined in WE BUILD's WP3 Technology and Standards group	Variation: EAA provider can be a bank or another Trust service provider (TSP)
10: DPC provisioning in EUDI Wallet	EUDIW	The DPC is provisioned and stored in the consumer's EUDI Wallet.		
11: DPC provisioning confirmation	EUDIW	The wallet confirms successful provisioning and displays the newly added payment credential to the user.		

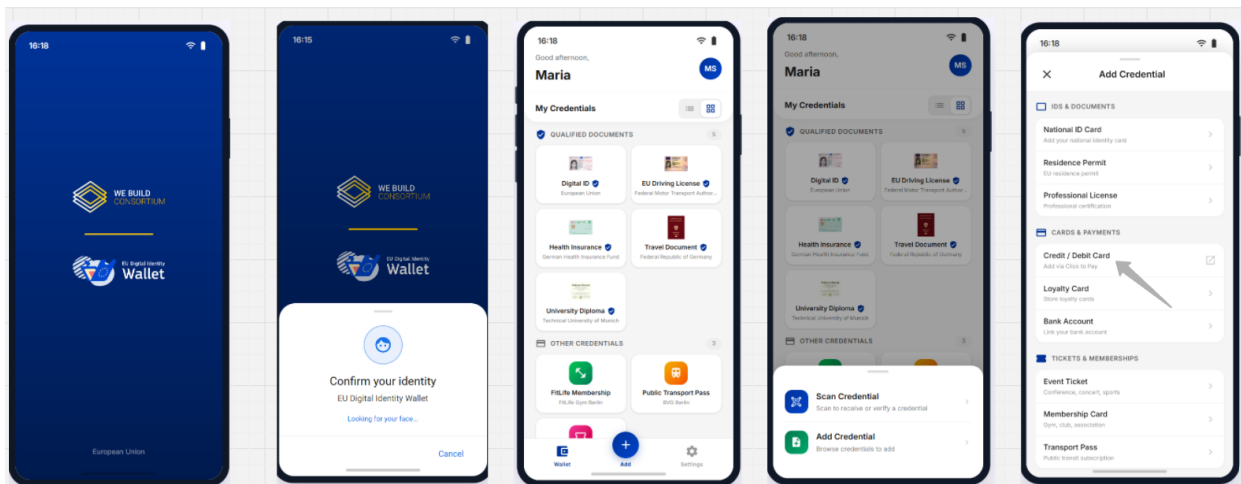
Post-Conditions:

- The consumer can visualize the DPC within their selected EUDI Wallet.
- The DPC is available for use in subsequent e-commerce transactions, including guest checkout scenarios.

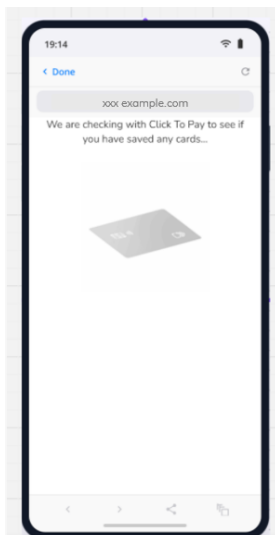
2.2.1.5 UX/UI examples

Mapped according to **section 2.2.1.4**

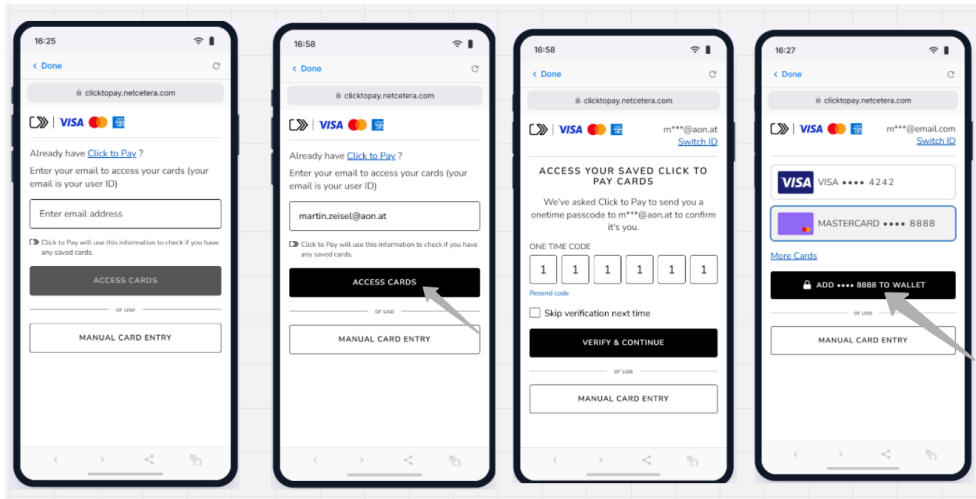
Flow Step 1



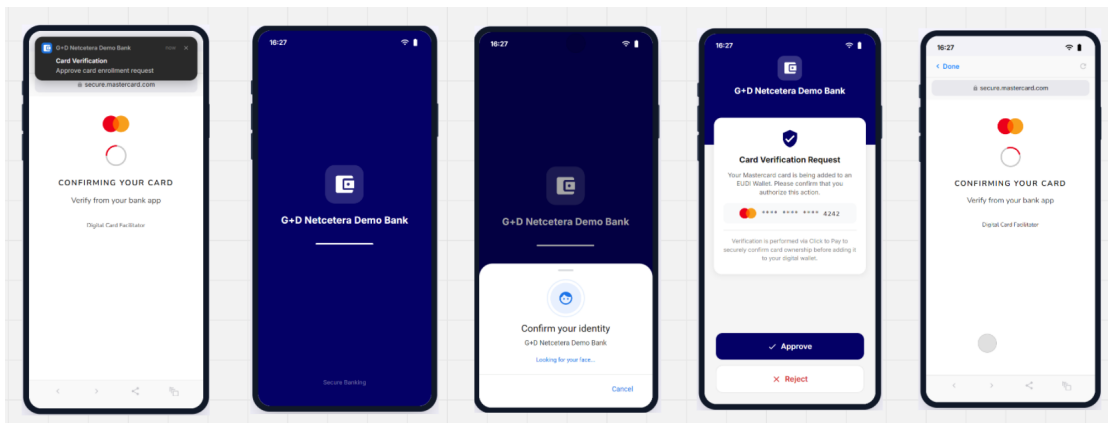
Flow Step 2 & 3:



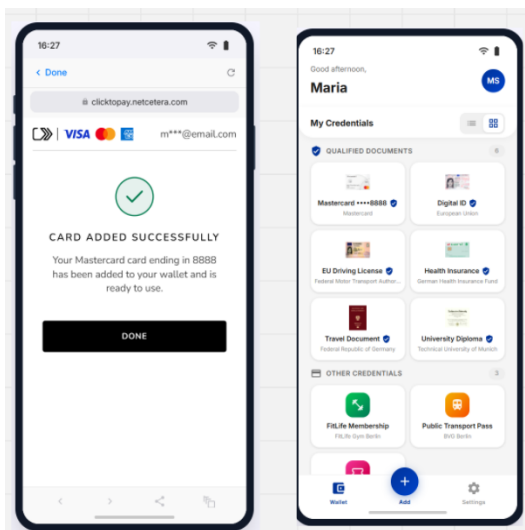
Flow Step 4 & 5



Flow Step 6



Flow Step 7 & 8



2.2.1.6 Sequence diagram

Two sequence diagrams are available for this flow. One of the two will be selected for piloting, with the final decision based on alignment with WP4 requirements and the outcome of the security vulnerability assessment.

1. DPC provisioning flow via Credential Issuance Facilitator (CIF)
 - EUDIW is integrated with CIF facilitating interaction with Card Network / EAA Provider
 - Please refer to Annex 2 in this document- **SD1 (A)**
 - Also, available on WE BUID Git Hub space; Access restricted to WE BUILD members: [wp3-technology-standards/sequence-diagrams/PA2/B.2 Cards Payment Initiation/b2-iss-pull+cif/b2-iss-pull+cif.md](https://github.com/wp3-technology-standards/sequence-diagrams/PA2/B.2%20Cards%20Payment%20Initiation/b2-iss-pull+cif/b2-iss-pull+cif.md) at main · webuild-consortium/wp3-technology-standards
2. Direct DPC provisioning flow with Card Network (EAA Provider) (No CIF)
 - EUDIW is directly integrated with Card Network
 - Please refer to Annex 2 in this document- **SD1 (B)**
 - Also, available on WE BUID Git Hub space; Access restricted to WE BUILD members: [wp3-technology-standards/sequence-diagrams/PA2/B.2 Cards Payment Initiation/b2-iss-pull+net/b2-iss-pull+net.svg](https://github.com/wp3-technology-standards/sequence-diagrams/PA2/B.2%20Cards%20Payment%20Initiation/b2-iss-pull+net/b2-iss-pull+net.svg) at main · webuild-consortium/wp3-technology-standards

2.2.2 MVP Flow 2: Presentation of DPC- Payment Initiation (Guest Checkout) using EUDIW

2.2.2.1 Main flow description

This flow describes a guest checkout card payment initiation where a consumer selects and presents a Digital Payment Credential (DPC) stored in their European Digital Identity Wallet (EUDI Wallet) on the same device as the merchant checkout environment.

The DPC presentation:

- Identifies the selected card for payment initiation, and
- Provides cryptographic proof of strong user authentication, device binding, and transaction intent, suitable for use as SCA evidence by issuers and payment networks.

Supported MVP environment:

- Mobile device (Android), same device

- Attestation: Digital payment Credentials (DPC)

Pilot Operating Model:

In this flow:

The merchant acts as the Relying Party (RP) and is responsible for requesting the Digital Payment Credential (DPC) as part of the payment flow.

Upon receiving the verifiable presentation from the wallet, the merchant forwards the DPC to designated card network:

- The Card Network acts as the Validator-TSP (Trust Service Provider), performing validation of the DPC (including cryptographic integrity and transaction binding) via its card network tokenization systems. This approach leverages existing merchant/PSP integrations with card network tokenization infrastructure, thereby minimizing additional implementation effort for merchants.
- The card tokenization system validates DPC, including its cryptographic integrity and transaction binding. Upon successful verification, the card network returns the relevant assurance data and transaction credentials (e.g., token, cryptogram) to the merchant/PSP for use in payment authorization.

Alternative implementation models, such as issuer or bank operated verification (e.g., the issuing bank or its authorized technology provider acting as the DPC verifier) are possible and can be explored out of the scope of this pilot.

Roles and Responsibilities (Pilot Scope):

Actors	Role/Acting as
Consumer	Holder
Bank	Card Issuer & ACS; ACS may be operated by bank or by an authorized technology provider acting on behalf of the bank.
Wallet	EU Digital Identity Wallet
E-commerce Merchant/PSP	Relying party
Card Network	Validator-TSP (Trust Service Provider); (DPC verifier)

2.2.2.2 Additional flows

The following variations may be supported in the pilot:

Flow	Short description
Variations	
Same device, Custom URI flows	The payment is initiated on a single device where the merchant checkout triggers the user's EUDI Wallet via a Custom URI deep link. The user is redirected from the browser/merchant app to the wallet for authentication and consent, after which the signed payment credential is returned to the merchant via a callback URI to complete the transaction
Exceptions	
No active DPC available	Payment initiation request fails. Merchant to display other payment options. If no active Digital Payment Credential (DPC) is available in the consumer's wallet, the payment initiation request fails at the platform/OS level. The merchant is then required to present alternative payment options to the user to complete the transaction.

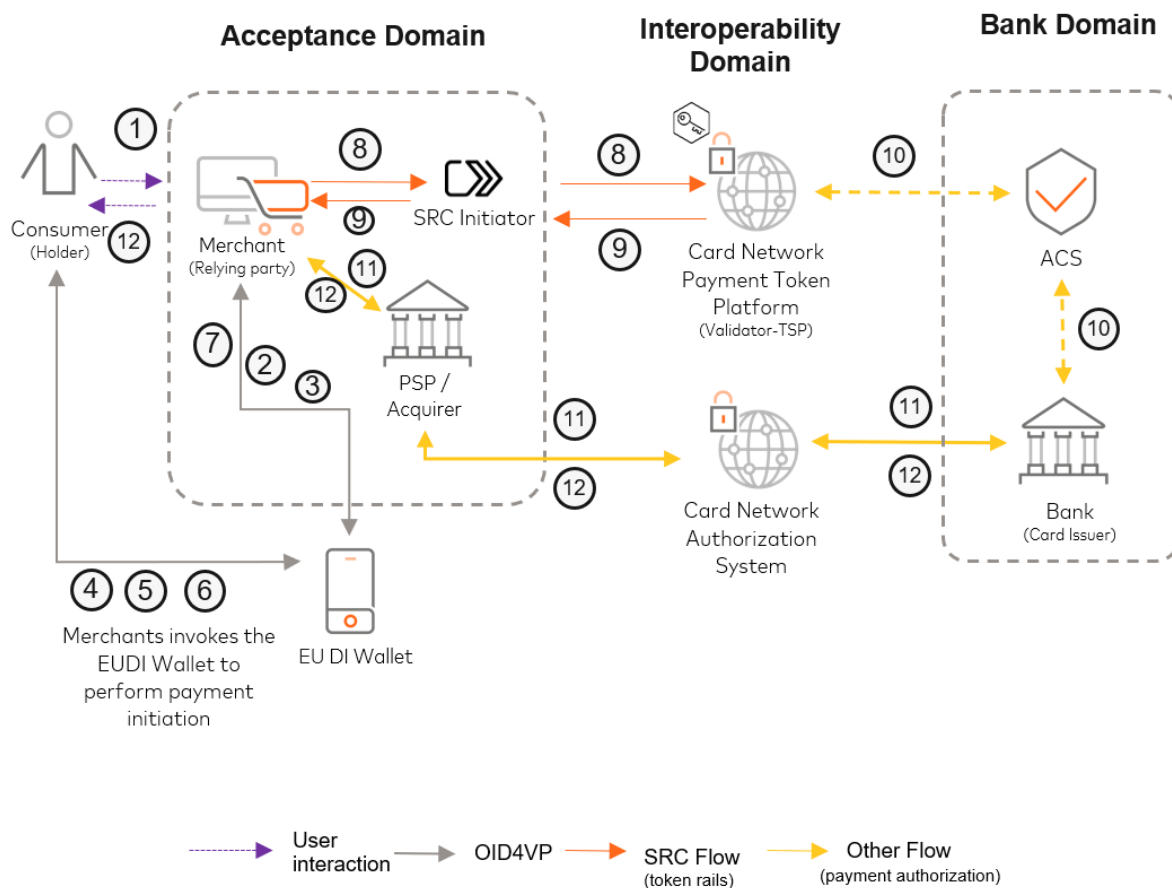
Variations assumption:

Two DPC presentation flows are considered within the scope of this pilot: MVP2 (Presentation of DPC- Payment Initiation) and MVP3 (Presentation of DPC- Payment Initiation with combined presentation). To keep the specifications unique and diverse across flows, the same-device variation is considered under MVP2, while cross-device variation is considered under MVP3. Each variation is applicable across both scenarios.

2.2.2.3 Pre-conditions

- The consumer has a valid Digital Payment Credential (DPC) stored in the EUDI Wallet app on their mobile device, issued through Flow1 (Provisioning of DPC through EUDIW).
- The merchant/PSP, wallet instance and consumer's browser support:
 - W3C Digital Credential API, and
 - OpenID4VP protocol for requesting DPC presentations
- The card referenced by the DPC is active and in good standing with the payment network's Token directory.

- The merchant PSP has connectivity to the relevant payment networks / acquirers to fetch DPC-derived transaction data and process authorization requests using these transaction data.
- The Merchant/PSP (Relying Party) and/or an intermediary acting on its behalf (Relying Party Intermediary), and the EU Digital Identity Wallet (EUDIW) provider, shall have their respective Trust Anchors registered and discoverable within the same Trust Framework. (Note: for this pilot the Trust framework will be issued and managed by the WP4 group).



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
1: Payment Initiation using EU Digital Identity Wallet	Merchant/PSP	On same mobile device, consumer accesses the merchant's website/app and adds items to the shopping cart. The merchant presents available payment options in checkout environment. The consumer selects 'EU Digital Identity Wallet' option (labelling indicative / subject to UX decisions)	A new EU Digital Identity wallet-based payment option is introduced in the merchant checkout page	
2. Credential Presentation Request using OpenID4VP protocol	Merchant/PSP	The merchant/PSP invokes the Digital Credentials API (navigator.credentials.get()), providing an OpenID4VP presentation request that specifies: - Required/Accepted credential type (e.g. Digital Payment Credential), - Transaction data (e.g. amount, currency, merchant name), - Relying party metadata		Variation: Instead of DC API custom URI can be used as a wallet invocation mechanism
3: Dynamic Linking	OpenID4VP Protocol	The OpenID4VP request cryptographically binds the DPC presentation to the specific transaction parameters, ensuring dynamic linking between user authentication and the payment		

		transaction.		
4.Platform's Response to OpenID4VP Request	Platform/OS	The platform / operating system presents a system payment sheet to the user. The payment sheet: • Displays transaction details (merchant, amount) • Displays the default DPC that satisfy the request. • The interface is credential-centric (no wallet selection).		Exception: In case no active DPC is found the Payment initiation request fails. Merchant to display alternate payment options. Variation (iOS): The interface displays the available wallets supporting the request on the device, enabling wallet selection prior to credential presentation.
5: DPC selection for payment	Consumer/Holder	On the system payment sheet, consumer selects the default DPC of preferred card to be used for this checkout.		In case where multiple DPCs are available, the consumer can select a DPC other than the default on their mobile device Variation (iOS): Consumer selects the desired DPC from the wallet interface.
6: Strong User Authentication	Platform/OS + EUDIW	The Platform / OS invokes the EUDI Wallet to obtain explicit user confirmation. The EUDI Wallet: • Displays the transaction details (e.g. merchant name, amount, card art). • Displays the verified status of the Merchant/PSP (Relying Party) or Relying Party Intermediary in		Variation (iOS): The consumer is already within the wallet interface when strong user authentication is requested. As a result, the platform does not perform a separate wallet invocation step, and user confirmation and SCA are completed directly within the wallet context.

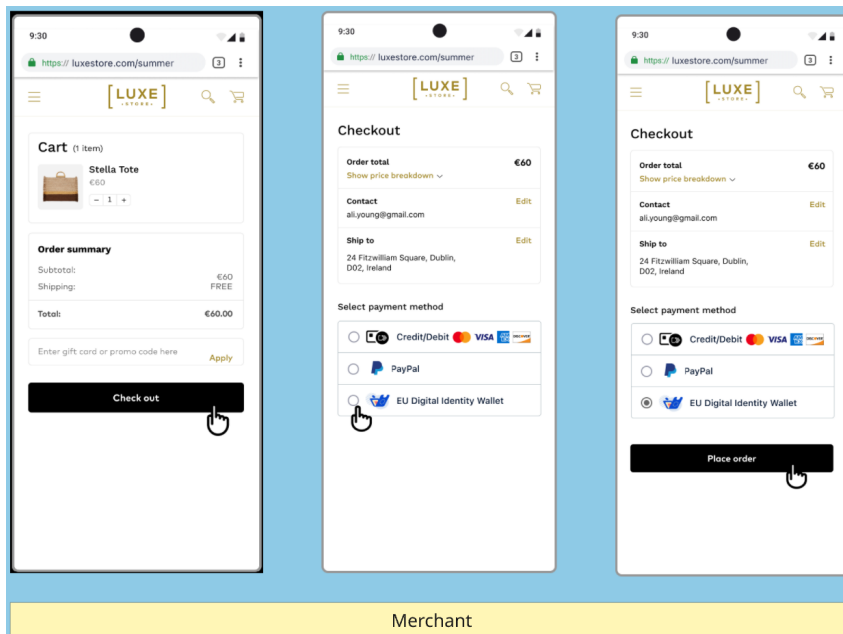
		accordance with the applicable Trust Framework. Requests for strong user authentication meeting regulatory SCA requirements (e.g. biometric or device PIN).		
7: EUDIW generates Verifiable Presentation and response via OpenID4VP	EUDIW	Upon successful user approval, the EUDI Wallet generates a verifiable presentation of the DPC and returns it to the Relying Party using OID4VP. The presentation includes: - A reference to the card / token (cloud token reference), - Key binding / proof of possession data, - Transaction-specific cryptographic evidence, as required.		
8: Relying Party OpenID4VP response processing and DPC submission to Validator-TSP for verification	Merchant/PSP	The merchant/PSP processes the OpenID VP presentation and sends the verifiable presentation to the card network tokenization systems.		
9: DPC validation and token response by Card Network	Card Network	The card network tokenization system acting as the Validator-TSP (DPC verifier): Verifies the		

		cryptographic validity of the OpenID4VP presentation - Validates transaction binding - Return the assurance data & transaction credentials (ex: token, cryptogram, etc.).		
10: Data only 3DS signalling for risk assessment	Merchant/PSP	(Optional) Depending on the card network tokenization system, the guest checkout flow may include a 3DS signalling or data-only exchange. This enables the issuer to receive transaction and risk signals without triggering a cardholder challenge, and to apply issuer-side risk assessment to approve or decline the transaction based on its internal decisioning.		
11: Payment authorization	Merchant	Merchant/PSP submits the payment authorisation request using the transaction credentials obtained on step 9		
12: Payment confirmation	Merchant	Upon successful authorisation (Card N/W and issuer), the merchant displays payment confirmation to the user on the website or app.		

2.2.2.5 UX/UI examples

MVP environment: Mobile device (Android), Same Device, With DC API

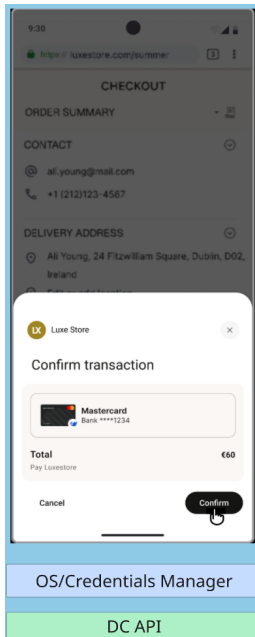
Flow Steps 1-3



Flow Steps 4 & 5 (2 Possibilities at this stage):

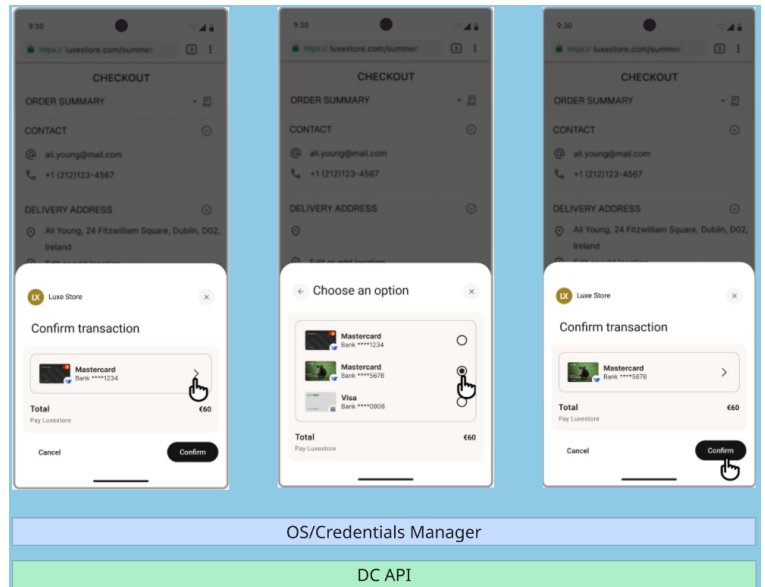
Possibility 1

Possibility 2

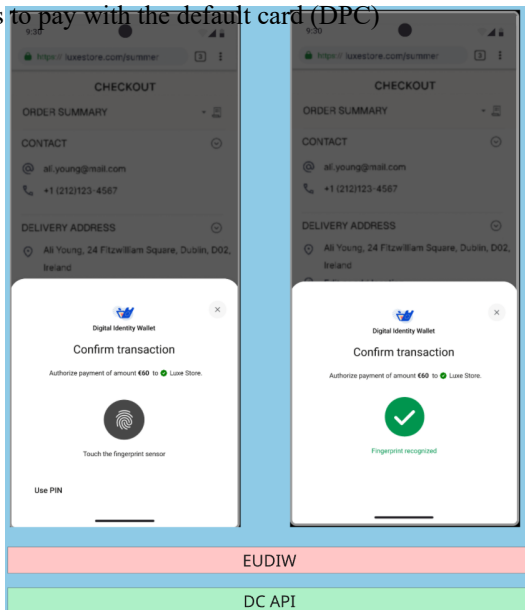


Flow Steps 6 & 7

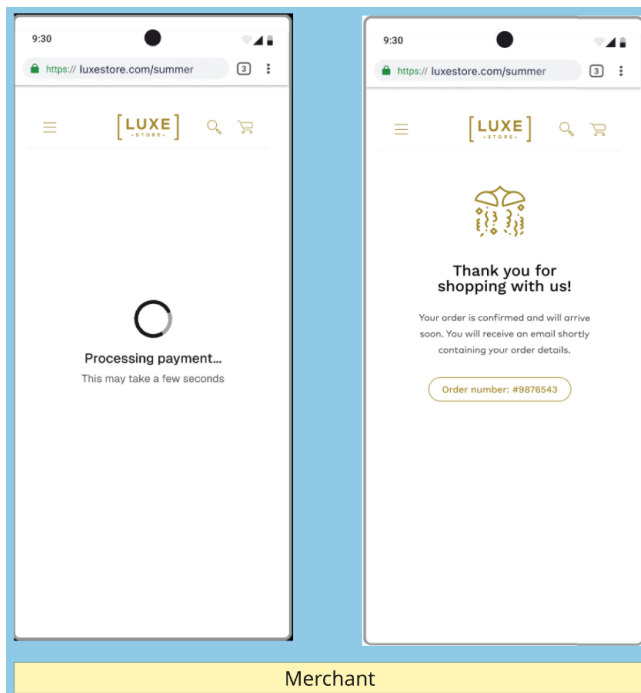
Consumer has a **single** card (DPC) available or wants to pay with the default card (DPC)



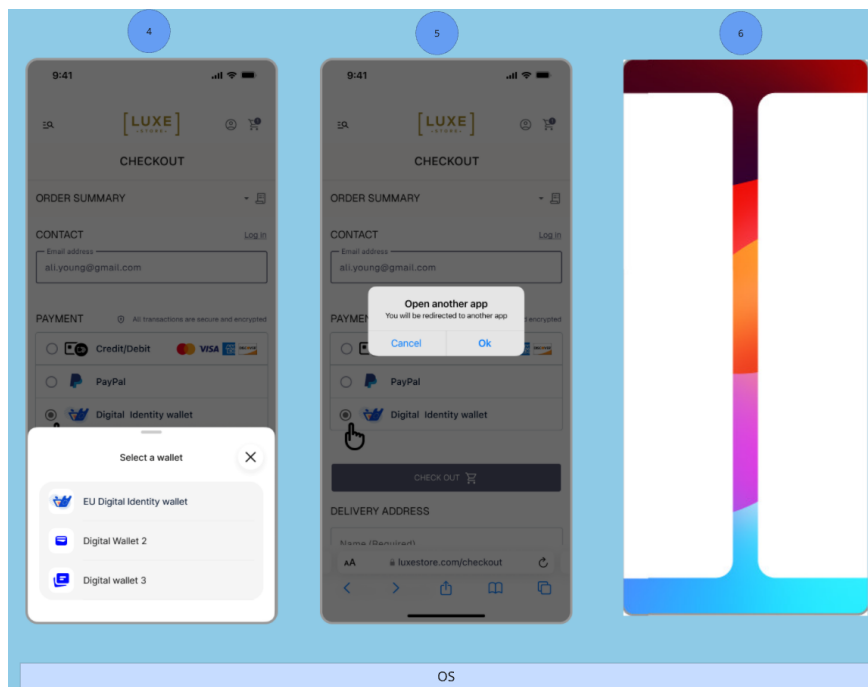
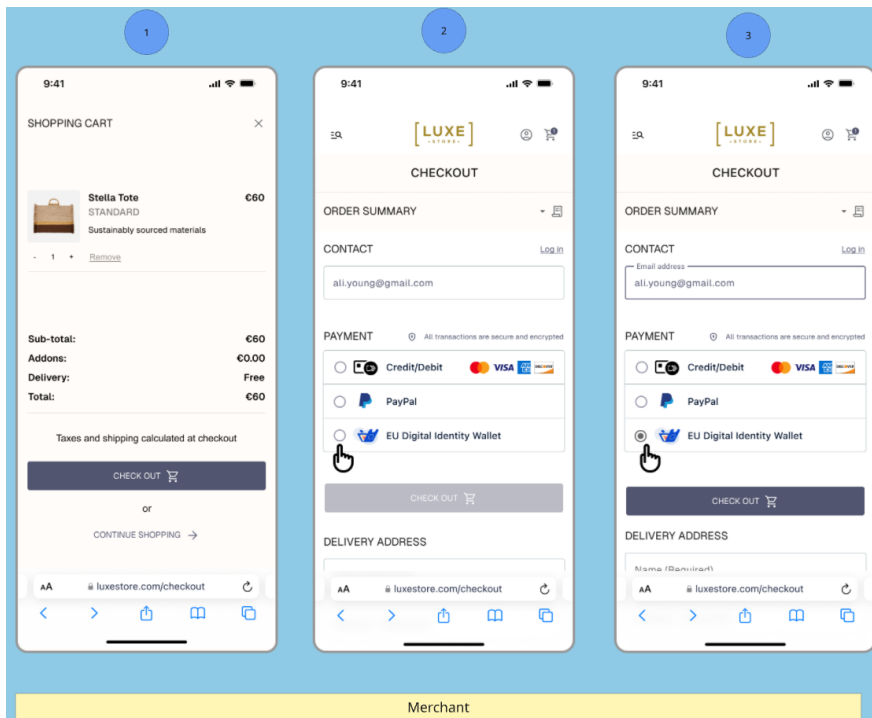
Consumer has **multiple** DPCs available and wants to pay with DPC other than the default DPC

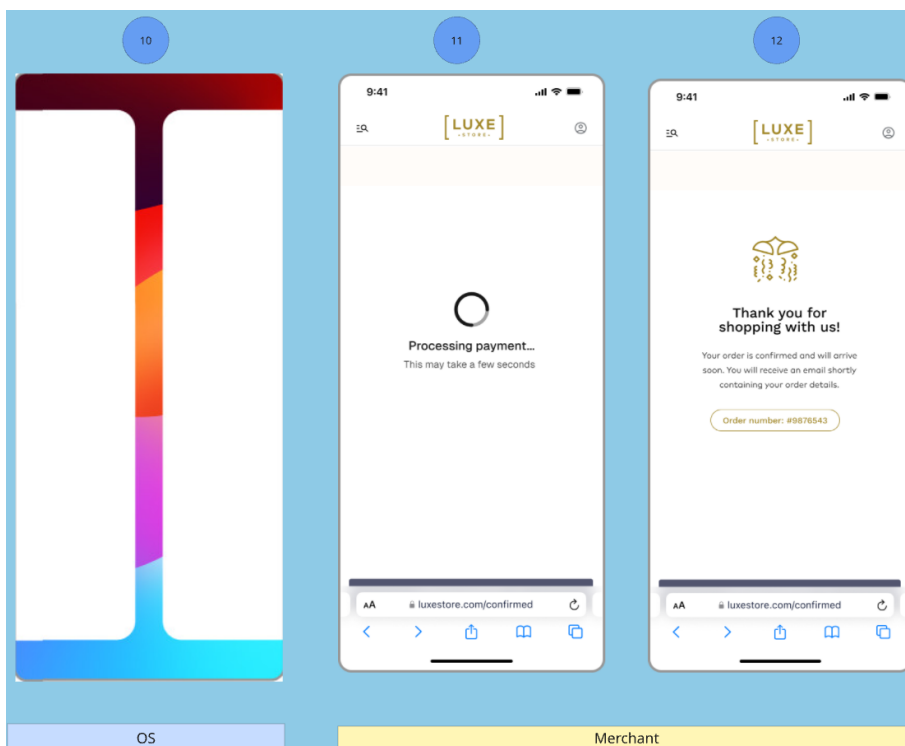
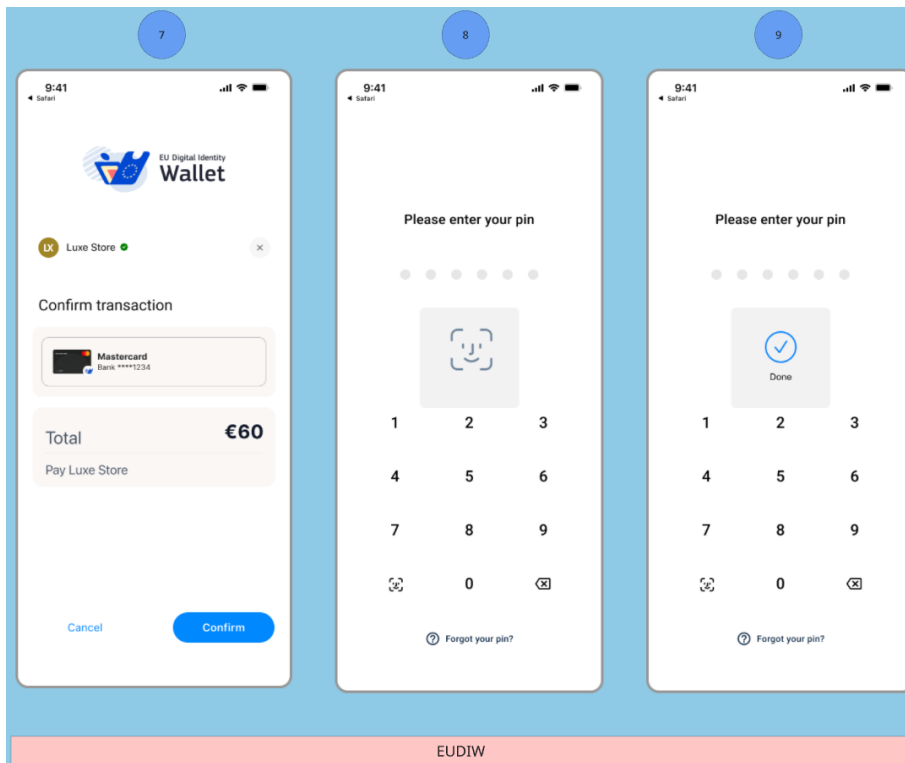


Flow Steps 8-12



Variation: Same device, iOS, Custom URI deep link





2.2.2.6 Sequence diagram

- Please refer to Annex 2 in this document- **SD 2**
- Also, available on WE BUID Git Hub space; Access restricted to WE BUILD members:: [wp3-technology-standards/PA2/B.2 Card Payment Initiation/b2-pre-agc at main · webuild-consortium/wp3-technology-standards](#)

2.2.3 MVP Flow 3: Presentation of DPC- Payment Initiation + Combined Presentation (Enhanced Guest Checkout)

2.2.3.1 Main flow description

This flow describes a guest checkout card payment initiation use case where a consumer selects and presents a Digital Payment Credential (DPC) together with a combined presentation of ‘proof of eligibility’ (as defined in section 1.2.1 of this document) e.g. age claim, Student ID, Loyalty card etc., stored in their European Digital Identity Wallet (EUDI Wallet) on the same device as the merchant checkout.

The DPC presentation:

- Identifies the selected card for payment initiation, and
- Provides cryptographic proof of strong user authentication, device binding, and transaction intent, suitable for use as SCA evidence by issuers and payment networks.

The ‘proof of eligibility’ presentation:

- Identifies the relevant attestation (e.g. age attribute, Student ID) for combined presentation with payment credential.
- Provides cryptographic proof of authenticity and integrity of the credential, issued by a trusted authority.
- Ensures consumer’s consent and transparency over which attributes are being disclosed as part of the transaction

Supported MVP environment:

- Mobile device (Android), same device
- Attestation: Digital payment Credentials (DPC)

Pilot Operating Model:

In this pilot flow:

The merchant acts as the Relying Party (RP) and is responsible for requesting the Digital Payment Credential (DPC) as part of the payment flow. In addition, the merchant/PSP may request one or more additional “proof of eligibility” credentials (e.g., age claims, student ID, loyalty card etc.) as part of the same DCQL request.

Upon receiving the verifiable presentation from the wallet, the following processing model applies:

- The merchant (or its designated intermediary service) acts as the verifier for “proof of eligibility” credentials, validating the presented attributes. Upon successful verification of the “proof of eligibility”, the merchant or PSP shall forward the Digital Payment Credential (DPC) to the Card Network for verification.
- The Card Network acts as the Validator-TSP (DPC verifier), performing validation of the DPC (including cryptographic integrity and transaction binding) via its tokenization systems. This approach leverages existing merchant/PSP integrations with card network tokenization infrastructure, thereby minimizing additional implementation effort for merchants.
- The card tokenization system validates DPC, including its cryptographic integrity and transaction binding. Upon successful verification, the card network returns the relevant assurance data and transaction credentials (e.g., token, cryptogram) to the merchant/PSP for use in payment authorization.

Alternative implementation models, such as issuer or bank-operated verification (e.g., the issuing bank or its authorized technology provider acting as the DPC verifier), are possible and can be explored out of the scope of this pilot.

Roles and Responsibilities (Pilot Scope):

Actor	Role/Acting as
Consumer	Holder
Bank	Card Issuer & ACS; ACS may be operated by bank or by an authorized technology provider acting on behalf of the bank.
Wallet	EU Digital Identity Wallet
E-commerce Merchant/PSP	Relying party & ‘proof of eligibility’ credential verifier

Card Network	Validator-TSP (Trust Service Provider); (DPC verifier)
--------------	--

2.2.3.2 Additional flows

Flow	Short description
Variations	
Cross device DC API (laptop +mobile)	The payment and ‘proof of eligibility’ verification is initiated across two devices, where the consumer accesses the merchant checkout on one device (e.g. desktop) and the EUDI Wallet is invoked on another (mobile).The merchant uses the Digital Credentials API to trigger the flow via QR code, enabling the wallet to authenticate the consumer and return the signed payment and ID credential to complete the transaction.
Exceptions	
No active DPC or ‘Proof of eligibility’ attestation available	Payment initiation or ‘proof of eligibility’ verification request fails. Merchant to display other payment options. If no active Digital Payment Credential (DPC) or ‘proof of eligibility credential is available in the consumer’s wallet, the request fails at the platform/OS level. The merchant is then required to present alternative payment or verification options to the user to complete the transaction.

Variations assumption:

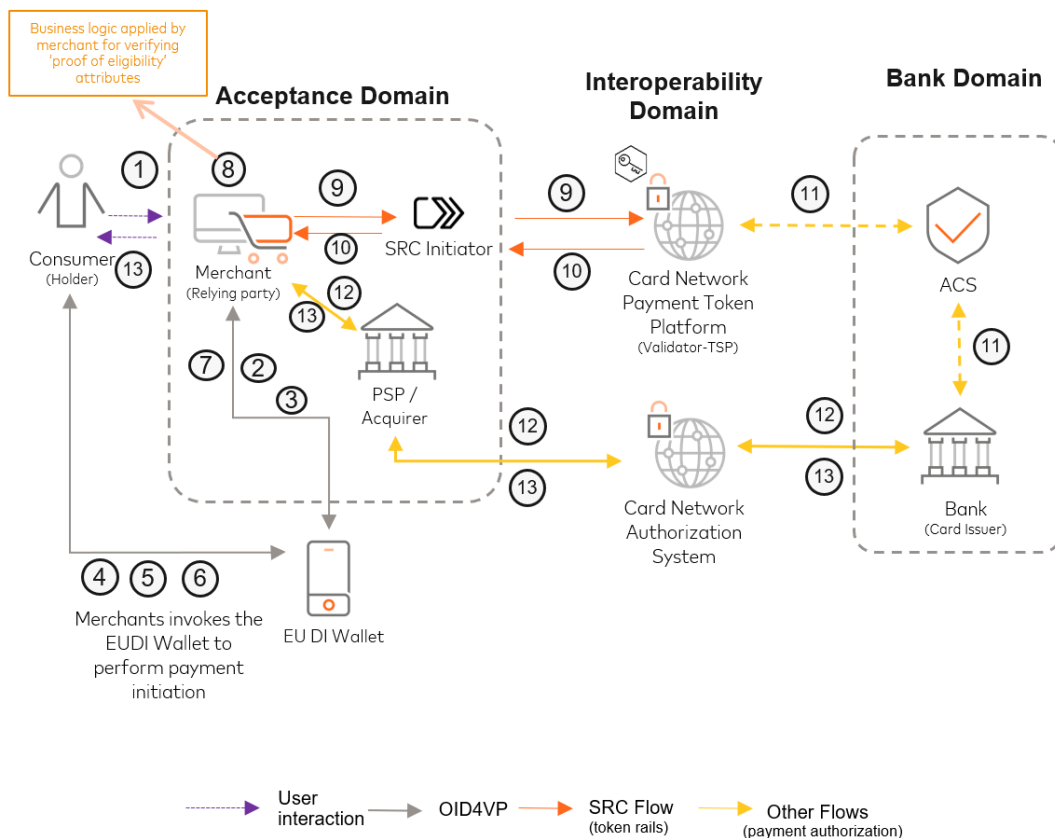
Two DPC presentation flows are considered within the scope of this pilot: MVP2 (Presentation of DPC- Payment Initiation) and MVP3 (Presentation of DPC- Payment Initiation with combined presentation). To keep the specifications unique and diverse across flows, the same-device variation is considered under MVP2, while cross-device variation is considered under MVP3. Each variation is applicable across both scenarios.

2.2.3.3 Pre-conditions

- The consumer has a valid Digital Payment Credential (DPC) stored in the EUDI Wallet app on their mobile device, issued through Flow 1 (Provisioning of DPC through EUDIW).
- The consumer has a valid attestation (e.g. PID, Student ID, Loyalty card etc.) issued and stored in the EUDI Wallet, capable of supporting ‘proof of eligibility’.
- The merchant/PSP supports:

- W3C Digital Credentials API, and
- OpenID4VP protocol for requesting combined presentation (DPC and ID attestations).
- The card referenced by the DPC is active and in good standing with the payment network's token directory.
- The merchant/PSP has connectivity to the relevant payment networks / acquirers to fetch DPC-derived transaction data and process authorisation requests using these data.
- The Merchant/PSP (Relying Party) and/or an intermediary acting on its behalf (Relying Party Intermediary) and EU DI Wallet (EUDIW) provider shall have their Trust Anchors registered and discoverable within the same Trust Framework. (Note: for this pilot the Trust framework will be issued and managed by the WP4 group).

2.2.3.4 Flow Steps



Trigger: The consumer proceeds to checkout on the merchant website and selects the option to pay using their EUDI Wallet.

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
1: Payment Initiation (combined) using EU Digital Identity Wallet	Merchant/PSP	On same device, consumer accesses the merchant's website/app and adds items to the shopping cart. The merchant presents available payment options in checkout environment. The consumer selects 'EU Digital Identity Wallet' payment option (labelling indicative / subject to UX decisions). The consumer is also required to present a 'proof of eligibility' (e.g. age verification or Student ID attestation) to prove eligibility as part of the combined presentation flow.	EU Digital Identity wallet-based payment option is introduced in the merchant checkout page	Variation: Cross device flow: The consumer accesses the merchant's website on a laptop and initiates the payment. For authentication, the consumer uses the EUDI Wallet on a mobile device. The merchant generates a QR code, which is scanned by the consumer using their mobile device to initiate the wallet interaction, with the Digital Credentials API acting as the invocation mechanism.
2: Credential Presentation Request using OpenID4VP protocol	Merchant/PSP	The merchant/PSP invokes the Digital Credentials API (navigator.credentials.get ()), providing an OpenID4VP presentation request that specifies: • Required/Accepted credential type (e.g. Digital Payment Credential). • Required 'proof of eligibility' attestation type (e.g. proof of age, student ID, loyalty card etc.) to		

		prove eligibility. - Transaction data (e.g. amount, currency, merchant name), - Relying party metadata .		
3: Dynamic Linking	OpenID4VP Protocol	The OpenID4VP request cryptographically binds the DPC and ‘proof of eligibility’ (e.g. proof of age, Student ID etc.) presentation to the specific transaction parameters, ensuring dynamic linking between user authentication, additional and the payment transaction.		
4.Platform’s Response to OpenID4VP Request	Platform/OS	The platform / operating system presents a system payment sheet to the user. The payment sheet: - Displays transaction details (merchant, amount) - Displays the default DPC and ‘proof of eligibility’ attestation (e.g. proof of age, Student ID etc) that satisfies the request. - The interface is credential-centric (no wallet selection).		In case no active DPC or ‘proof of eligibility’ attestation is found the payment initiation request fails. Merchant to display other payment options.
5:DPC selection for payment	Consumer/ Holder	Consumer selects the default DPC of preferred card to be used for this checkout.		
6: Strong User Authentication	Platform/OS + EUDIW	The Platform / OS invokes the EUDI Wallet to obtain explicit user confirmation. The EUDI Wallet: - Displays the transaction details (e.g. merchant name, amount, card art) - Displays the verified status of the Merchant/PSP		

		(Relying Party) or Relying Party Intermediary in accordance with the applicable Trust Framework. Requests for strong user authentication meeting regulatory SCA requirements (e.g. biometric or device PIN).		
7: EUDIW generates Verifiable Presentation and response via OpenID4VP	EUDIW	Upon successful consumer approval, the EUDI Wallet generates a combined verifiable presentation (DPC and ‘proof of eligibility’ attestation) and returns it to the Relying Party using OID4VP. The presentation includes: - A reference to the card / token (cloud token reference). ‘Proof of eligibility’ attributes - Key binding / proof of possession data, - Transaction-specific cryptographic evidence, as required.		
8: Relying Party OpenID4VP response processing	Merchant/PSP	The merchant/PSP parses and processes the OpenID VP request containing the combined credential set. Business logic is then applied, whereby the merchant verifies the ‘proof of eligibility’ attributes to confirm that the user meets the		If the ‘proof of eligibility’ verification fails. The payment flow is terminated by merchant.

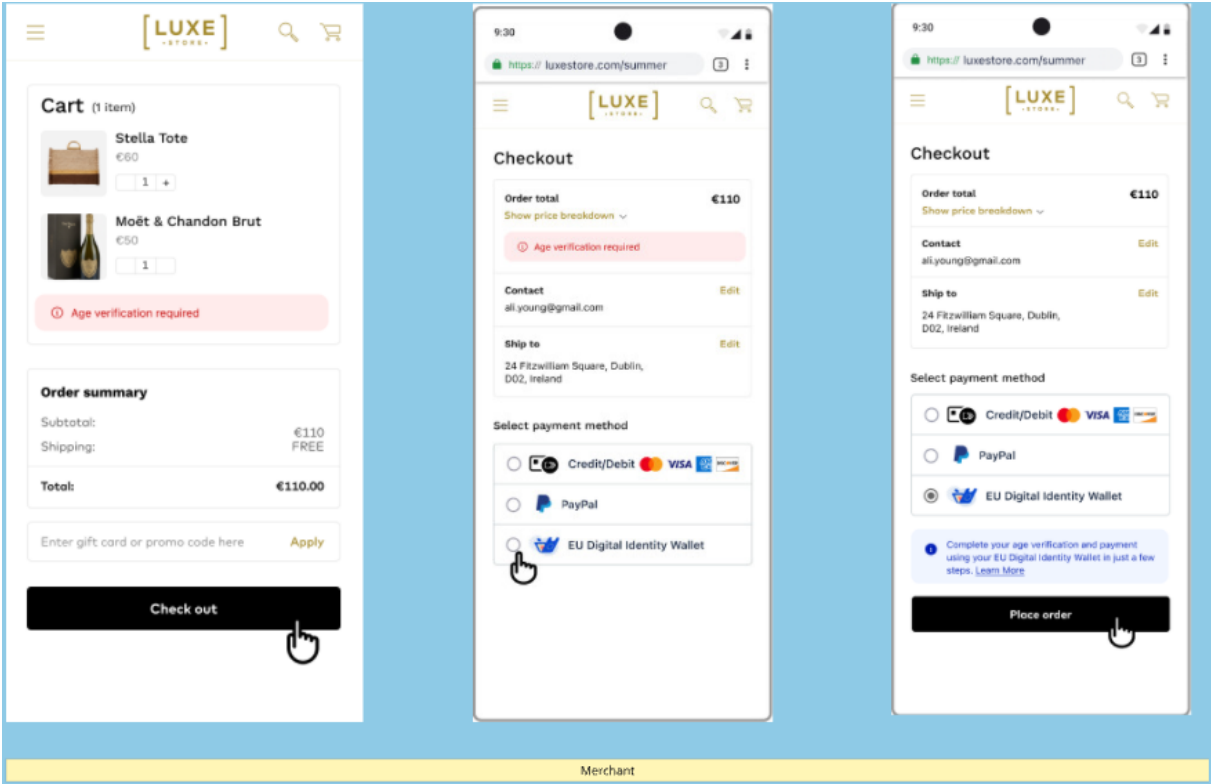
		required criteria for the specific use case. Upon successful verification, the merchant proceeds with the subsequent payment processing steps (9-13)		
9: DPC submission to Validator-TSP for verification	Merchant/PSP	The merchant/PSP sends the verifiable presentation (DPC only) to the card network tokenization systems.		
10: DPC validation and token response by Card Network	Card Network	The card network tokenization system acting as the Credential (DPC) Verifier: • Verifies the cryptographic validity of the OpenID4VP presentation • Validates transaction binding • Return the assurance data & transaction credentials (ex: token, cryptogram, etc.).		
10: Data only 3DS signalling for risk assessment	Merchant/PSP	(Optional) Depending on the card network tokenization system, the guest checkout flow may include a 3DS signalling or data-only exchange. This enables the issuer to receive transaction and risk signals without triggering a cardholder challenge, and to apply issuer-side risk assessment to approve or decline the transaction based on its internal decisioning.		
12: Payment authorisation	Merchant/PSP	Merchant/PSP submits the payment authorisation request using the transaction credentials obtained on		

		step 10		
13: Payment confirmation	Merchant/PSP	Upon successful authorisation (Card N/W and issuer), the merchant displays payment confirmation to the user on the website or app.		

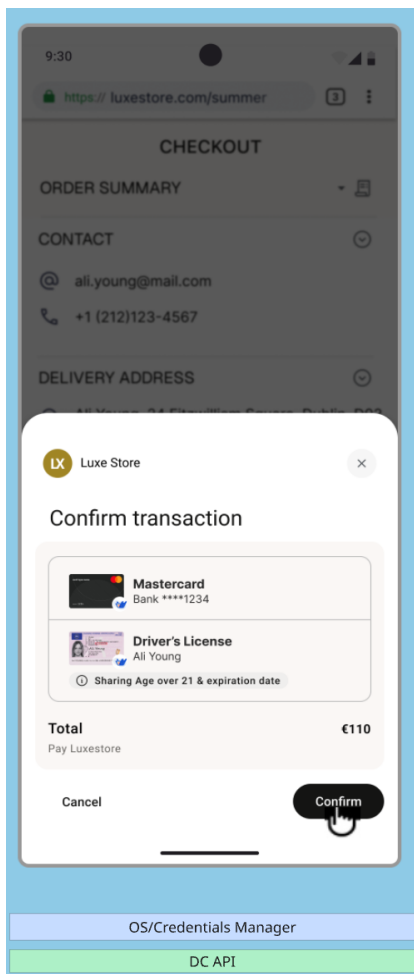
2.2.3.5 UX/UI examples

MVP environment: Mobile device (Android), Same Device, With DC API

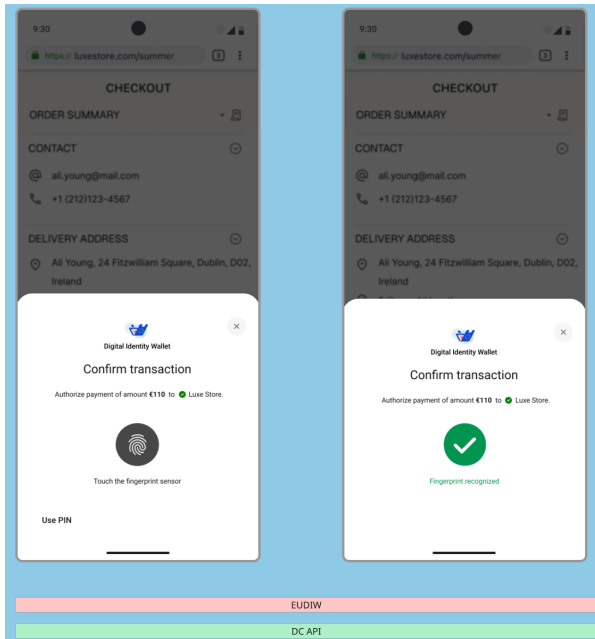
Flow Steps 1-3



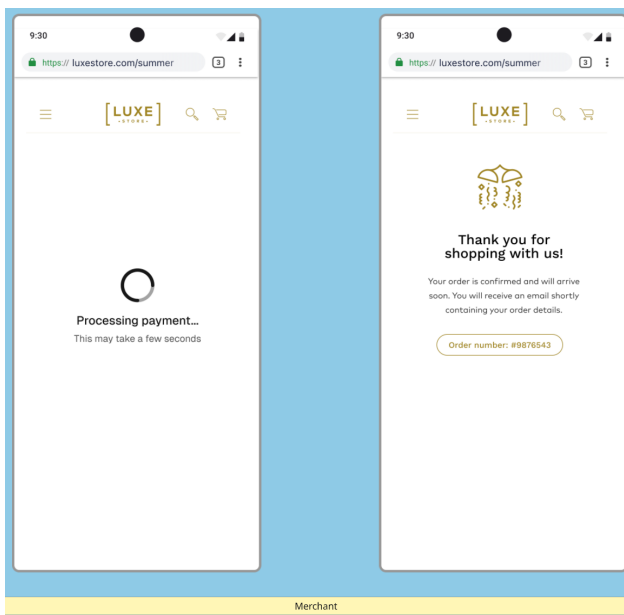
Flow step 4 & 5



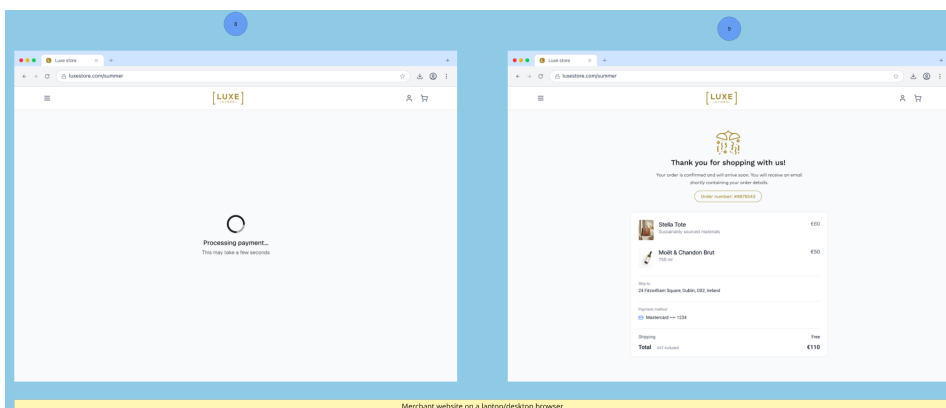
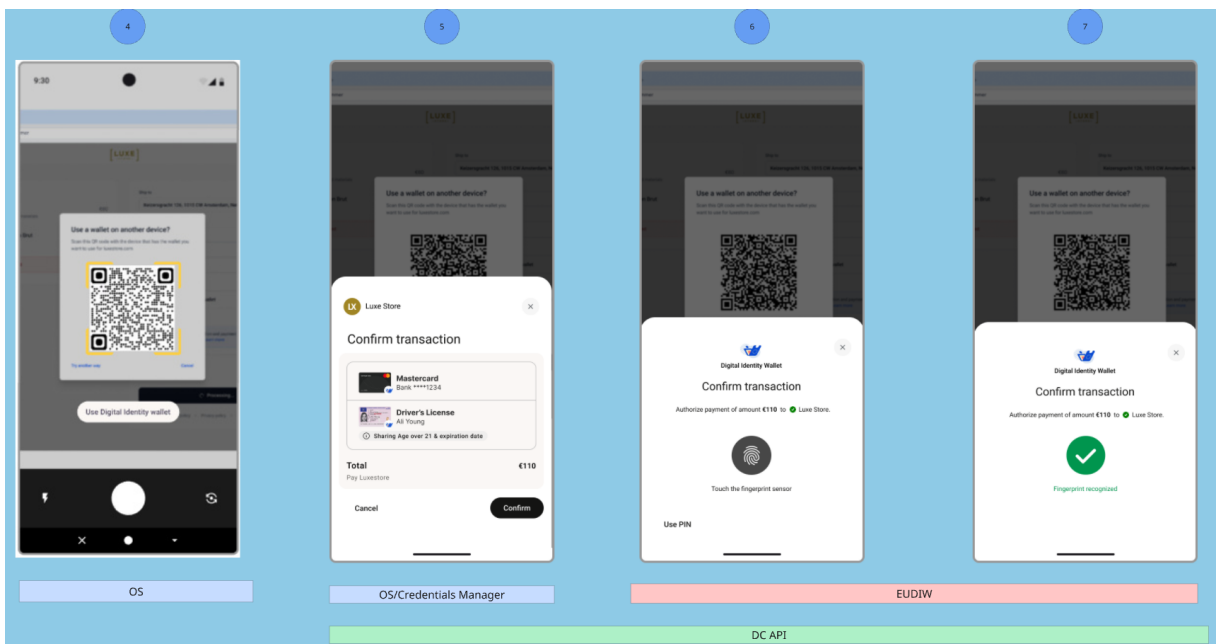
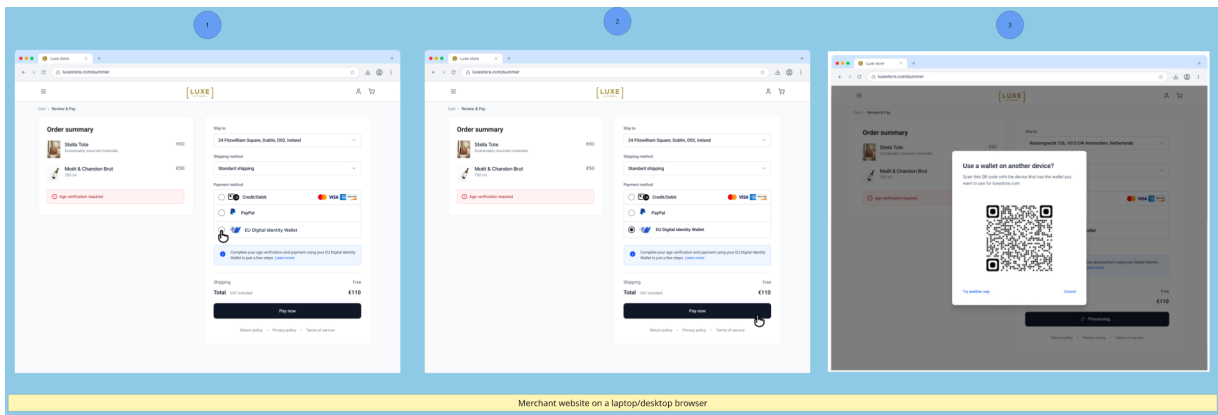
Flow steps 6 & 7



Flow steps 8-13



Variation: Cross device[Laptop (Chrome) & Mobile (Android)], With DC API



2.2.3.6 Sequence diagram

- Please refer to Annex 2 in this document- **SD 3**
- Also, available on WE BUID Git Hub space; Access restricted to WE BUILD members:[wp3-technology-standards/sequence-diagrams/PA2/B.2 Cards Payment Initiation/b2-pre-agc+combined_presentation/b2-pre-agc+combined_presentation.md at main · webuild-consortium/wp3-technology-standards](#)

2.3 EUDIW checkout experience: Integration Options

With the intention of addressing the challenges highlighted in Section 2.3.1, Scenario B2 explores two complementary integration options for presenting the EUDI Wallet as a payment initiation method within the merchant checkout environment. The primary objective is to support flexibility in merchant integration while ensuring alignment with existing checkout ecosystems.

The options are:

1. **Integration Option 1 - Embedded within existing card-based checkout mechanisms**

An integrated EUDI Wallet payment option within existing and proven card-based payment mechanisms (e.g. manual card entry and Click to Pay interfaces). This approach leverages established, instrument-driven checkout flows to embed EUDI Wallet-based payment initiation within familiar and widely adopted user journeys.

2. **Integration Option 2 - Standalone EU Digital Identity Wallet-based option**

A new and standalone “EUD Digital Identity Wallet” payment option presented directly at the merchant checkout. This approach enables a wallet-centric experience, allowing merchants to request and users to present payment credentials from their EUDI Wallet.

This dual approach reflects the objective of providing merchant and PSP flexibility, enabling them to select the integration model that best fits their checkout design, user experience strategy, and supported payment credential types.

Within the scope of the pilot, the intention is to evaluate the most viable integration approach, taking into account partner feedback, technical feasibility, and implementation readiness. The selection of the preferred approach(s) will therefore be guided by ongoing partner discussions and

practical considerations observed during the pilot, with the objective of identifying scalable and user-friendly integration patterns for broader ecosystem adoption.

2.3.1 Integration options: Explained

2.3.1.1 Integration option 1: Embedded within existing card-based checkout mechanisms

2 options possible here:

1.1 For Click to Pay enabled merchants

- **Option 1.1 (A.):** ‘EU Digital Identity Wallet’ option integrated with Click to Pay
- **Option 1.1 (B.):** DPC discovery in Click to Pay

1.2 For non-Click to Pay enabled merchants

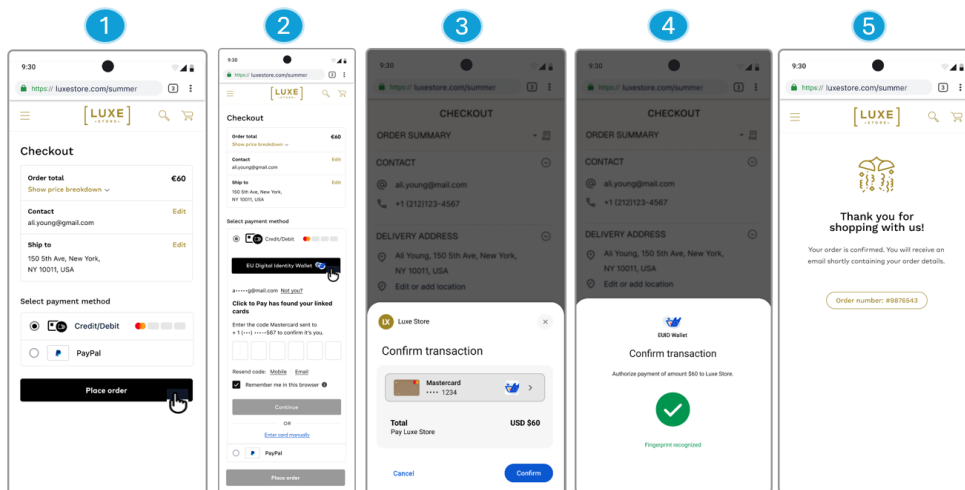
- **Option 1.2** ‘EU Digital Identity Wallet’ option integrated with ‘Credit/Debit’

These options have been explained below:

Option 1.1 (A.) ‘EU Digital Identity Wallet’ option integrated with Click to Pay

GOAL: Merchant checkout (**For C2P merchants**) using Click to Pay profile to select “use your EUDI Wallet” to surface DPC card credentials only. Subjected to standardization

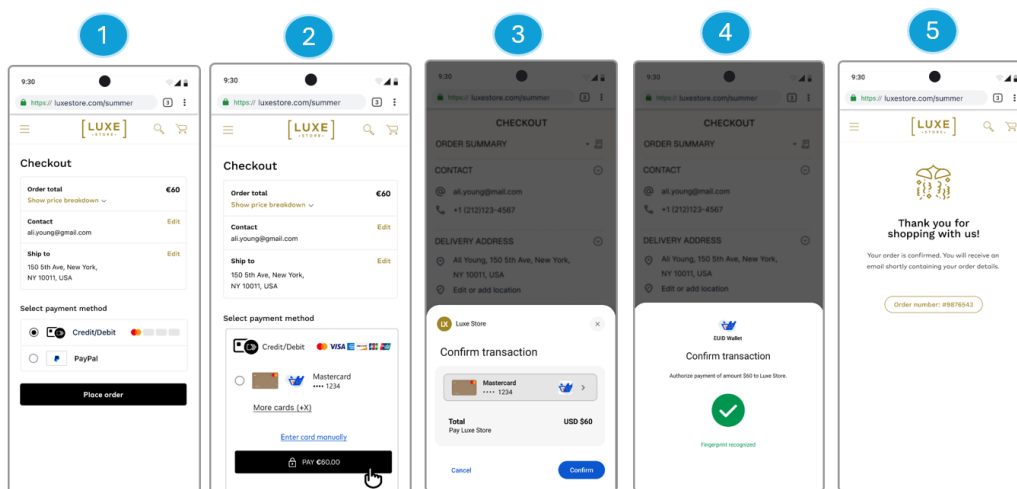
1. User select Click to Pay (C2P) checkout in the merchant.
2. C2P profile is loaded presenting log in screen AND a new “EU Digital identity Wallet” button.
3. DC API is invoked and payment sheet is shown by device OS.
4. User confirms the disclosure of the DPC by authenticating using the available methods provided by the wallet (e.g. device biometrics).
5. Merchant completes the remaining Authentication process and completes checkout



Option 1.1 (B.) DPC discovery in Click to Pay

GOAL: Merchant checkout (for C2P merchants) using consumers Click to Pay profile, which discovers all known DPCs stored in the different wallets (using new SRC lookup capabilities-subjected to standardization and industry alignment)

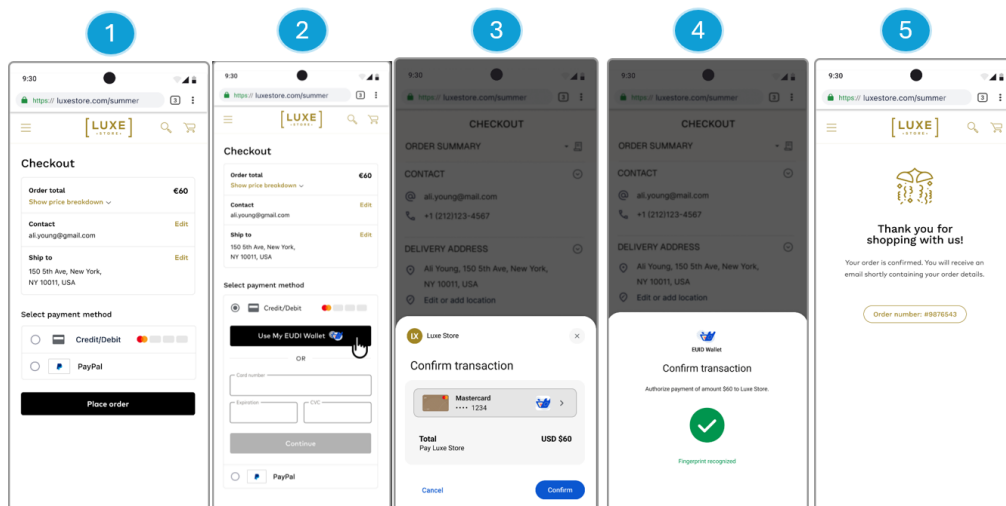
1. User select Click to Pay (C2P) checkout in the merchant.
2. C2P profile is loaded and available DPCs discovered, being presented to the user in C2P frame.
3. DC API is invoked and payment sheet is shown by device OS.
4. User confirms the disclosure of the DPC by authenticating using the available methods provided by the wallet (e.g. device biometrics).
5. Merchant completes the remaining Authentication process and completes checkout



Option 1.2. ‘EU Digital Identity Wallet’ option integrated with ‘Credit/Debit’

GOAL: Merchant checkout (for Non C2P merchants) using Debit/Credit default option to surface DPC card credentials.

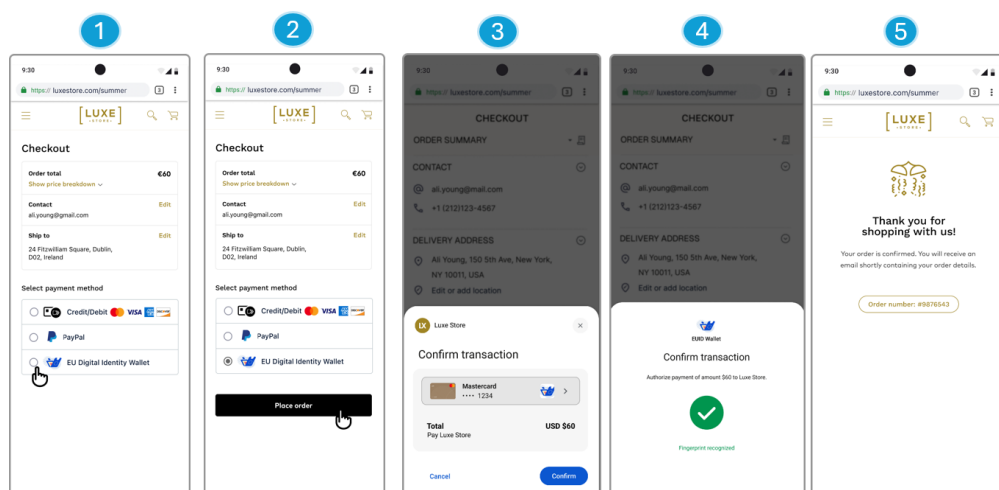
1. User select Credit/Debit as payment method
2. The Merchant or his PSP/Acquirer present the manual card entry option as usual AND a new “EU Digital Identity Wallet” button
3. DC API is invoked and payment sheet is shown by device OS.
4. User confirms the disclosure of the DPC by authenticating using the available methods provided by the wallet (e.g. device biometrics).
5. Merchant completes the remaining Authentication process and completes checkout



2.3.1.2 Integration Option 2 - Standalone wallet-based option

GOAL: Merchant checkout standalone EU Digital Identity Wallet option to surface DPC card credentials.

1. User select Click to Pay (C2P) checkout in the merchant.
2. C2P profile is loaded presenting log in screen AND a new “EU Digital identity Wallet” button.
3. DC API is invoked and payment sheet is shown by device OS.
4. User confirms the disclosure of the DPC by authenticating using the available methods provided by the wallet (e.g. device biometrics).
5. Merchant completes the remaining Authentication process and completes checkout



2.4 Challenges and barriers

2.4.1 Wallet discovery and branding on merchant checkout page

Wallet discovery and branding on the merchant checkout page is a significant challenge, as merchants may need to support 27+ EU Digital Identity Wallets issued across Member States. Presenting multiple wallets on the checkout page risks visual clutter, consumer confusion, and increased checkout friction, particularly in the absence of a unifying brand or standardized discovery mechanism. This challenge is further compounded by the need to manage user choice between card-based and account-based payment options (as defined in the A2 scenario), merchant scheme acceptance preferences, and the requirement to determine whether a Digital Payment Credential (DPC) already exists for the user before displaying an appropriate wallet or payment initiation option.

2.4.2 W3C Digital Credential API Maturity and Support

While W3C Digital Credential APIs (DC API) offer a more seamless and standardised wallet invocation experience, it's standards are still evolving. Further the practical availability of DC API depends on operating system support, browser capabilities and wallet provider maturity.

Deep-link invocation mechanisms are currently more widely supported but may result in less consistent user experiences across platforms.

2.4.3 DPC Schema Standardization

Standardisation of the Digital Payment Credential (DPC) schema under EMVCo is still in progress, which presents challenges for Scenario B2 pilot. This ongoing evolution limits the ability to rely on stable, production ready specifications and may require interim or pilot specific adaptations until DPC standards reach greater maturity and adoption.

2.5 Working Assumptions

2.5.1 Standards Maturity (DPC, DC API)

The standardisation of the Digital Payment Credential (EMVCo) schema and the DC API (W3C) is still ongoing in respective standardization organizations. As a result, pilot implementations will rely on draft, evolving, or constrained versions of these specifications. Ecosystem compatibility will therefore be validated at a pilot level, rather than reflecting full production-scale readiness.

2.5.2 W3C DC API considered as primary invocation mechanism

The same-device web checkout flow SHALL leverage the W3C Digital Credential API (DC API) as the primary invocation mechanism.

In cases where DC API is not supported by the browser or operating system, alternative invocation mechanisms (custom URI schemes) shall be used as fallback options.

For the purposes of this pilot, it is assumed that sufficient support for DC API will be available on Android devices within the pilot timeframe. Accordingly, pilot implementations shall be primarily conducted using Android devices with an option to use iOS devices for custom URI flows.

2.5.3 Trust Infrastructure availability

The pilot assumes a partial or simulated trust infrastructure. In particular, key ecosystem participants are expected to rely on the Trust List simulation provided by WP4 to validate attestations. While this dependency is accepted as a pilot-specific constraint, it is recognised as a risk in terms of production realism and scalability, especially for cross-border scenarios.

2.5.4 PID availability

PID availability is assumed for the purposes of the pilot; however, it will not be issued by a government authority, due to limited Government body representation within the WE BUILD consortium. Instead, Person Identification Data (PID) will be issued within WP4 to enable testing of the Scenario B2 flows. This approach is accepted as a pilot-specific assumption, but it does not represent a production-grade, government-issued PID model

2.5.5 Consumer identification:

For the purposes of this pilot, the consumer SHALL be an existing customer of a participating issuing bank and shall already hold a valid and active payment card issued by that bank.

It is further assumed that the consumer's identity has been previously verified by the issuing bank in line with applicable regulatory requirements, and that this existing relationship will be leveraged for participation in the pilot and representation within the EUDI Wallet.

3 Roles and participants

3.1 Roles represented in the scenario

Roles represented in the scenario:

- **Banks:**
 - Bank 1 – Country A
- **Relying Parties:**
 - Online Merchant 1 – Country A
 - Online Merchant 2- Country B
- **Wallet Providers:**
 - Country A
- **Holder:** Country A Natural Person, existing client of Bank 1 with an existing bank payment card, using an EU Digital Identity Wallet provided by the user's country wallet or a private wallet provider

In addition of eIDAS 2.0 roles mentioned above, below suggested key technology partners would also be required to support the scenario:

- Bank partners:
 - ACS provider
 - Card network as EAA provider
- Merchant partners:
 - PSP/Card Acquirer
 - Card Network as Validator-TSP (Trust Service Provider) – (*DPC verifier*)
 - Intermediary (e.g. Technology providers assisting merchants (Relying Party) with wallet interactions, generating merchant callbacks etc.)
- Wallets:
 - Credential Issuance Facilitator

3.2 Scenario roles and participants

Roles relevant for this scenario with identified pilot partners. Note that the roles primarily active in the use case are mentioned.

Primary role	UC partner Name	Country
User of EUDI Wallet	OP Bank (user)	Finland
Bank	OP Bank	Finland
Relying Party	Cyclades Fast Ferries + University of Aegean	Greece
	Google	Finland
EAA provider	Mastercard	N/A
Validator-TSP	Mastercard	N/A
Credential Issuance Facilitator	G+D Netcetera	N/A
ACS (Bank partner)	Worldline	Finland
	Entersekt	
PSP (Merchant partner)	Worldline	Greece

3.3 Additional roles and partners

Partners that primarily work in WP4 participate in piloting this scenario.

Primary role	UC partner Name	Country	Wallet
EUDI Wallet provider	iGrant.io	FIN	NW
	Walt.id	FIN	NW
	Google	FIN	NW
PID Provider	Aricoma		

3.4 Target country combinations

Target country combination / cross border definition

- Issuing country = Bank location
- RP country = Merchant location

	Issuing country						
Relying Party country		AT	BE	DE	FI	GR	CZ
	AT						
	BE						
	DE						
	FI				Yes		
	GR				Yes		
	CZ						

4 Attestations

4.1 Introduction

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	WP4	(Confirmed),	• PID to be issued in the EUDIW to

	credential containing core identity attributes of a natural person, such as: • Given name / family name • Date of birth • Unique personal identifier • Nationality PID is issued by a PID provider (typically a member state authority/ member state designated authority)		Participating issuing bank countries,	make it a 'Valid' EUDIW instance. • PID can be used for age verification for combined presentation scenario (but this may require a separate POA attestation). • Can be optionally used during DPC issuance.
Student ID attestation	The StudentID Attestation is an attestation provided by an authentic source such as a university, higher-education institution, or an authorised academic identity provider. The attestation proves that a natural person is (or was, depending on the validity period) affiliated with an educational organisation in a student capacity, and enables relying parties to verify student status and selected identity attributes using the European Digital Identity Wallet (EUDI Wallet).	GR		•
Loyalty Card attestation	The Ferry Loyalty Card Attestation is an attestation provided by a ferry operator to identify registered customers participating in a loyalty or frequent traveller program.	GR		•

4.3 Created attestations in the scenario

Attestation name	Short description	For Countries	Applicable domain standards
Digital Payment Credentials (DPC)	The DPC is a structured, selectively disclosable representation of a digitized	FIN	EMVCo

	payment card. It enables wallets to present card-related attributes, such as network, last four digits, opaque card ID or Payment Account Reference (PAR), without exposing sensitive PAN or token data. The Card DPC Attestation can be used for payment authentication and authenticated guest checkout use-cases.		
--	--	--	--

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	MoSCoW prioritization
User of EUDI Wallet	Have an active Natural Person EU Digital Identity Wallet installed and operational.	M
	Completed account registration on EUDIW application including PID registration	M
	Has a valid and active payment card issued by an issuer (Bank).	M
	Complete all required authentication steps- ID&V (DPC issuance flow) and biometric based SCA (Payment initiation flow)	M
	Accept issuer T&Cs for using card in EUDIW (displayed during flow)	C
	Have a valid 'proof of eligibility' attestation issued in wallet for combined payment initiation flow.	M
Bank	Consumer identification for pilot. Must be a customer of the bank.	M
	Issue a valid payment card to the user. This can be done as part of pilot, or an existing issued card can be used.	M
	Support delegation of DPC issuance to Card Network	M

	Have connectivity with card network token platform (e.g. SRC)	M
	Registration with the WE BUILD Trust Framework	C
	Provide T&Cs governing card use in EUDIW	S
	Align with PSD2 requirements via 3DS based authentication for issuance flow	M
Merchant/ Intermediary	Introduce 'EU Digital Identity Wallet' payment option in the checkout environment	M
	Support DC API and Custom URI based invocation mechanisms	M
	Generate a combined presentation request where the DPC and the additional 'proof of eligibility' credential are requested within the same checkout/payment context. Generate a wallet presentation request for the DPC, including the payment context required by the pilot.	M
	Bind the DPC presentation request to the merchant transaction data, including at least merchant identifier, amount, currency, transaction/session ID and payment reference.	M
	Receive and process the wallet presentation response and verify that the DPC presentation and /or 'proof of eligibility' presentation are consistent with the expected transaction context and business logic (wherever applicable)	M
	Apply business logic based on the 'proof of eligibility' credential before payment verification step.	M
	Forward the DPC and transaction information to card network tokenization system for verification	M
	Forward the validated DPC-derived payment information to the PSP/acquirer/card network flow for payment authorisation	M

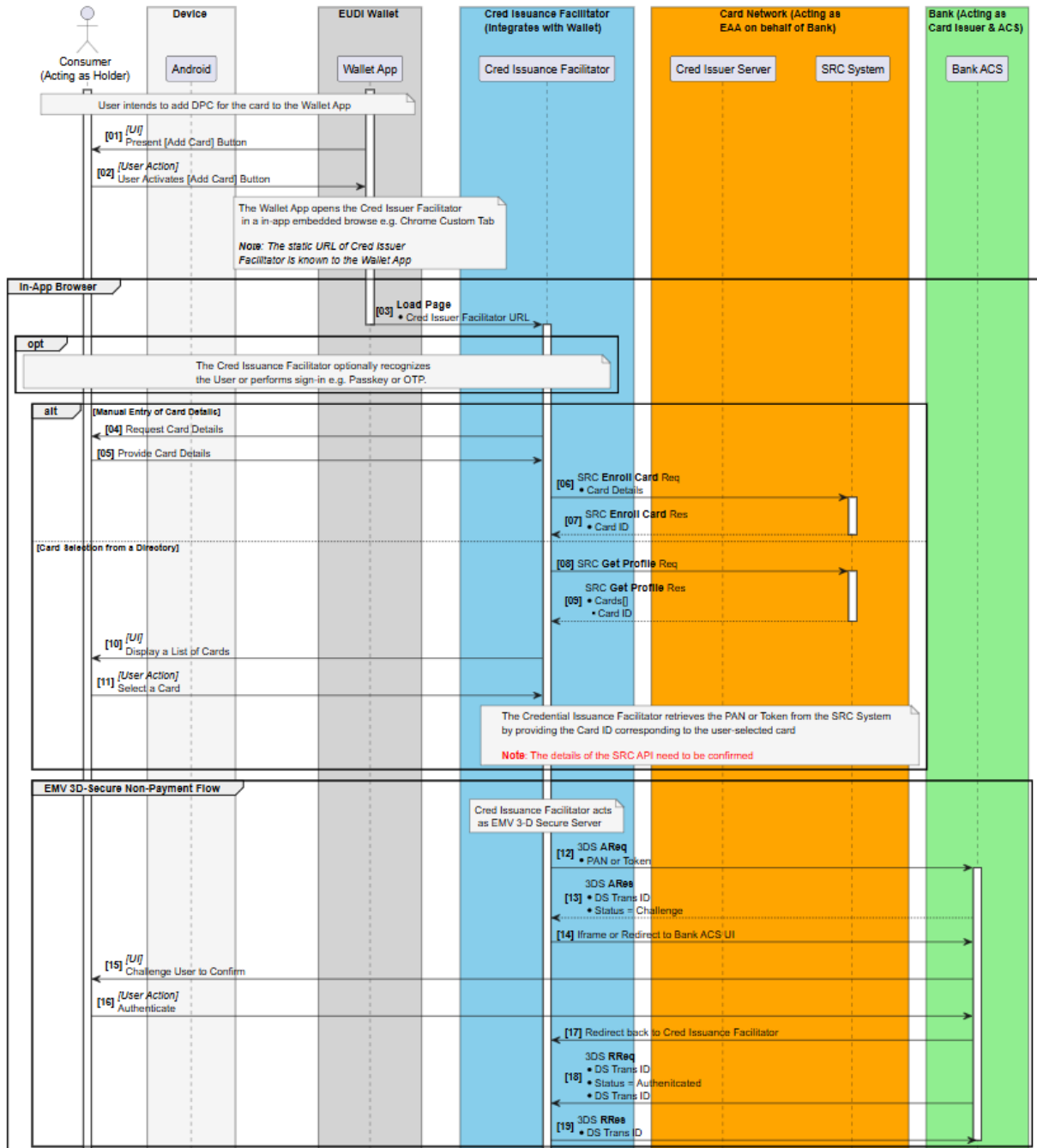
	Handle wallet cancellation, timeout, invalid presentation, declined payment and fallback to alternative payment methods.	M
	Define the outcome when one part of the combined presentation succeeds and another fails, e.g. valid DPC but invalid ID credential, valid ID but declined payment, or user cancellation.	M
EUDI Wallet provider	Provide EUDIW instance compliant with the WE BUILD conformance specifications.	M
	Registration of EUDIW instance with WE BUILD Trust Framework	M
	Allow user to initiate card-based credential issuance from the wallet environment (e.g. via 'Add a card' or 'Credit/Debit' options)	M
	Support both DC API and custom URI (deep link) based invocation mechanism	M
	Support DPC (SD-JWT) attestation provisioning and storage	M
	Integrate with Credential Issuance Facilitator or EAA provider or Banks (based on implementation choice) end points to initiate credential (DPC) issuance	M
	Share Wallet Unit Attestations as part of the issuance flow. WUA will be verified by the EAA provider before DPC issuance	M
PID Provider	No scenario specific requirements	
EAA provider (Card network)	Registration with WE BUILD Trust Framework as an EAA provider	M
	Support connectivity between card network token platform (e.g. SRC) and Bank	M
	Support connectivity between Card network token platform with Credential Issuance Facilitator to support DPC provisioning	S
	Issue Digital Payment Credential in Holder's EUDIW in SD-JWT VC format on behalf of bank (card issuer)	M

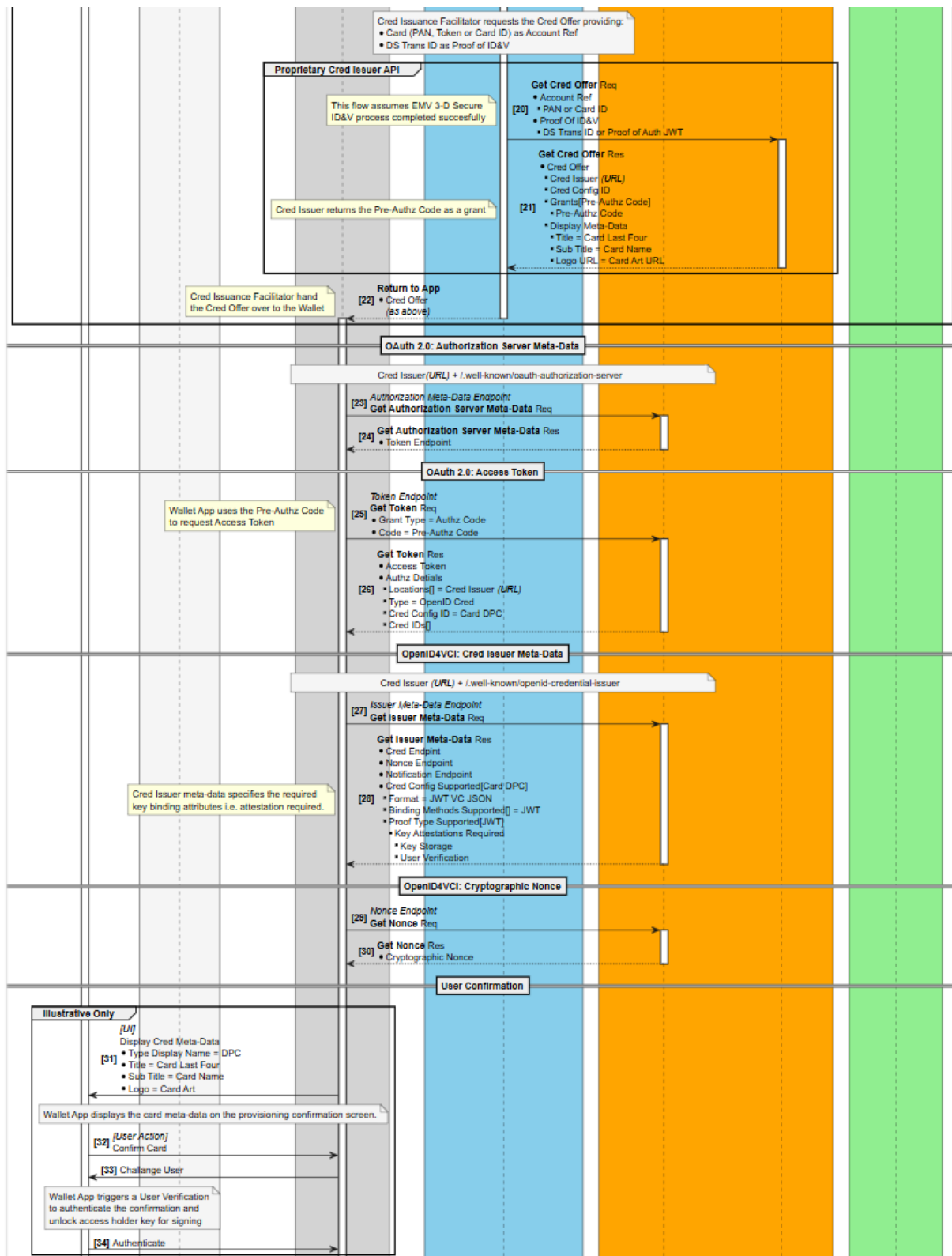
	Existing agreement between Bank and card network tokenization system has been updated to include provisions covering the use of card network tokenization system for EUDI Wallet based card credential creation.	C
Validator-TSP (Card network)	Support connectivity between card network token platform (e.g. SRC) and Merchant/PSP	M
	Verify Digital Payment Credential (SD-JWT) and transaction binding received from Merchant/PSP	M
	Return assurance data and transaction credentials back to Merchant/PSP	M
	Facilitate the payment authorization flow between Merchant/PSP and issuer	M
	Registration with WE BUILD Trust Framework as a TSP	C

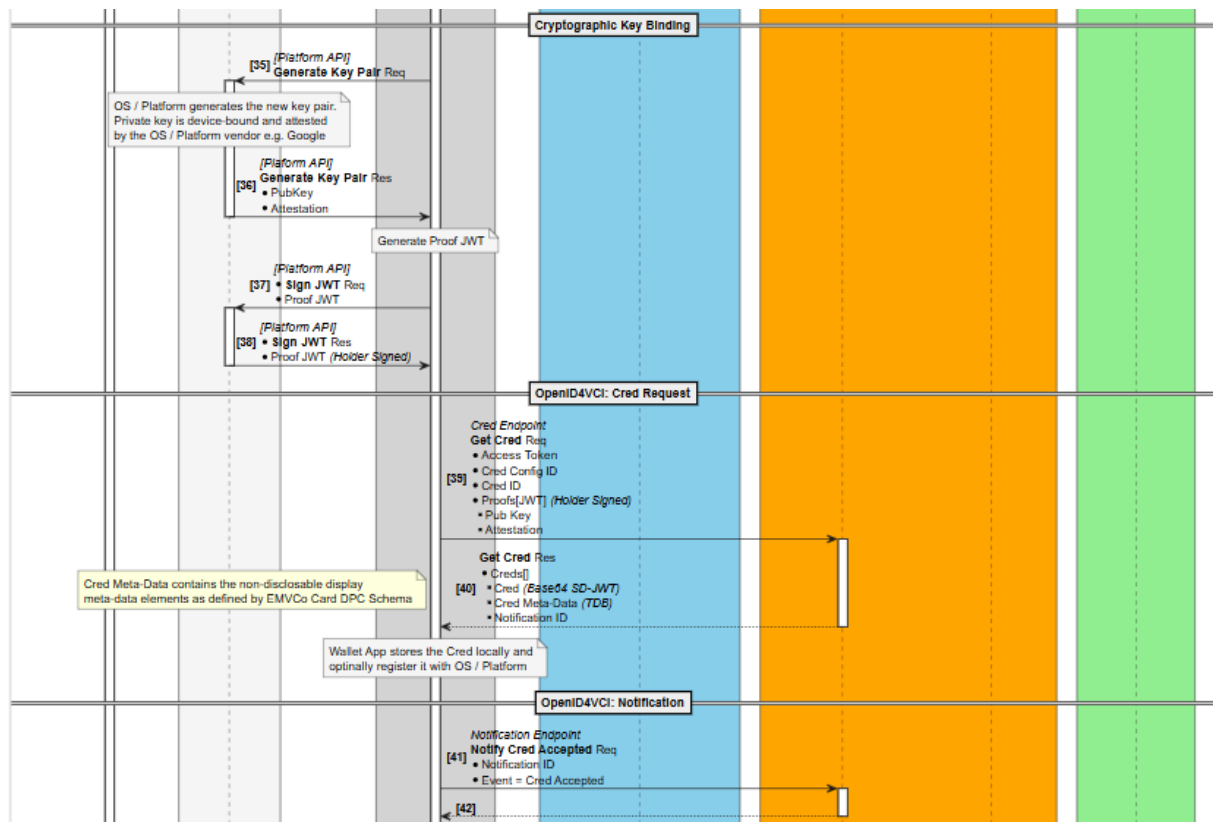
Annex 2 Sequence Diagrams

SD1(A): MVP Flow 1: Provisioning of DPC through EUDIW facilitated by Credential Issuance Facilitator

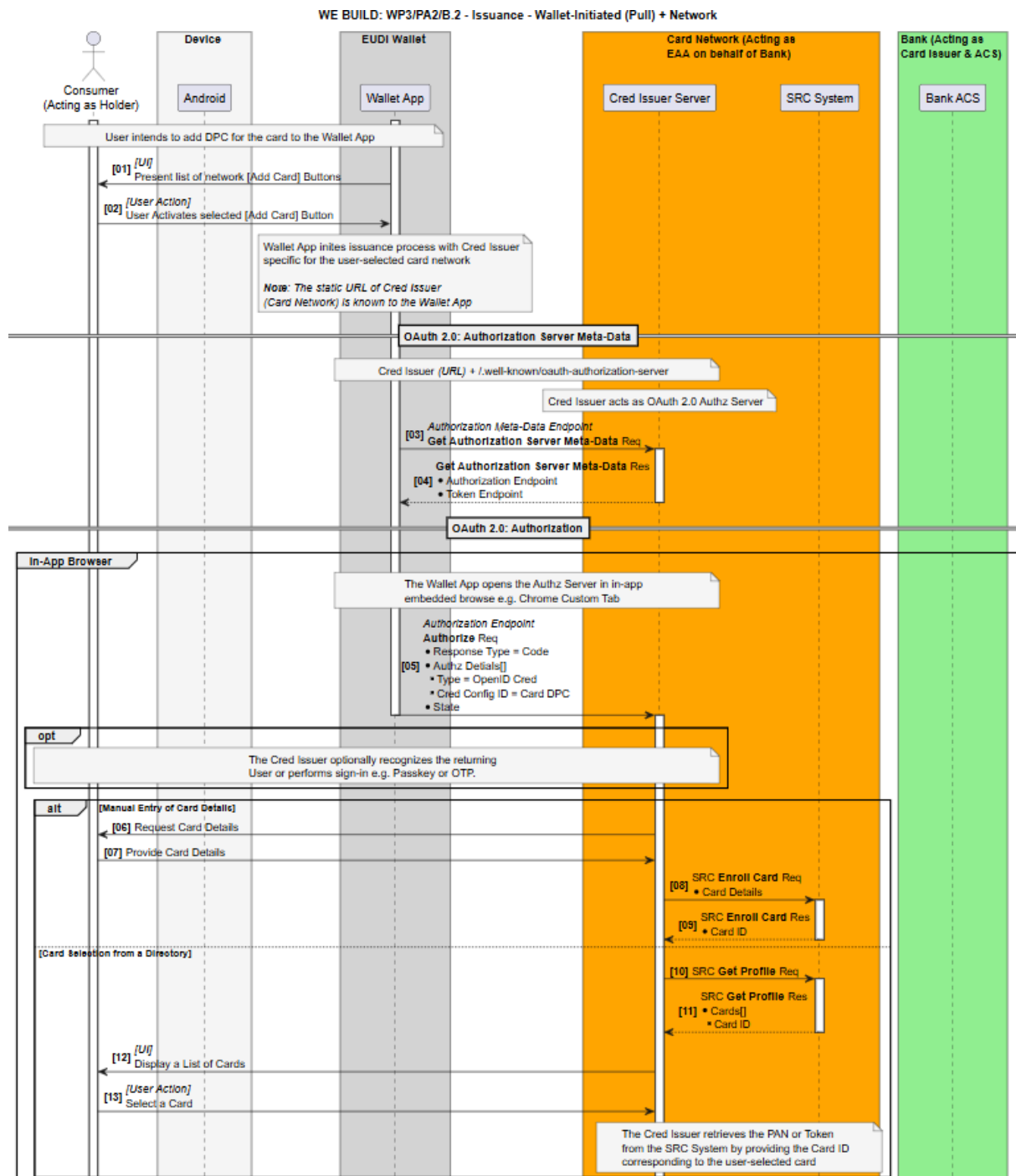
WE BUILD: WP3/PA2/B.2 - Issuance - Wallet-Initiated (Pull) + Cred Issuance Facilitator

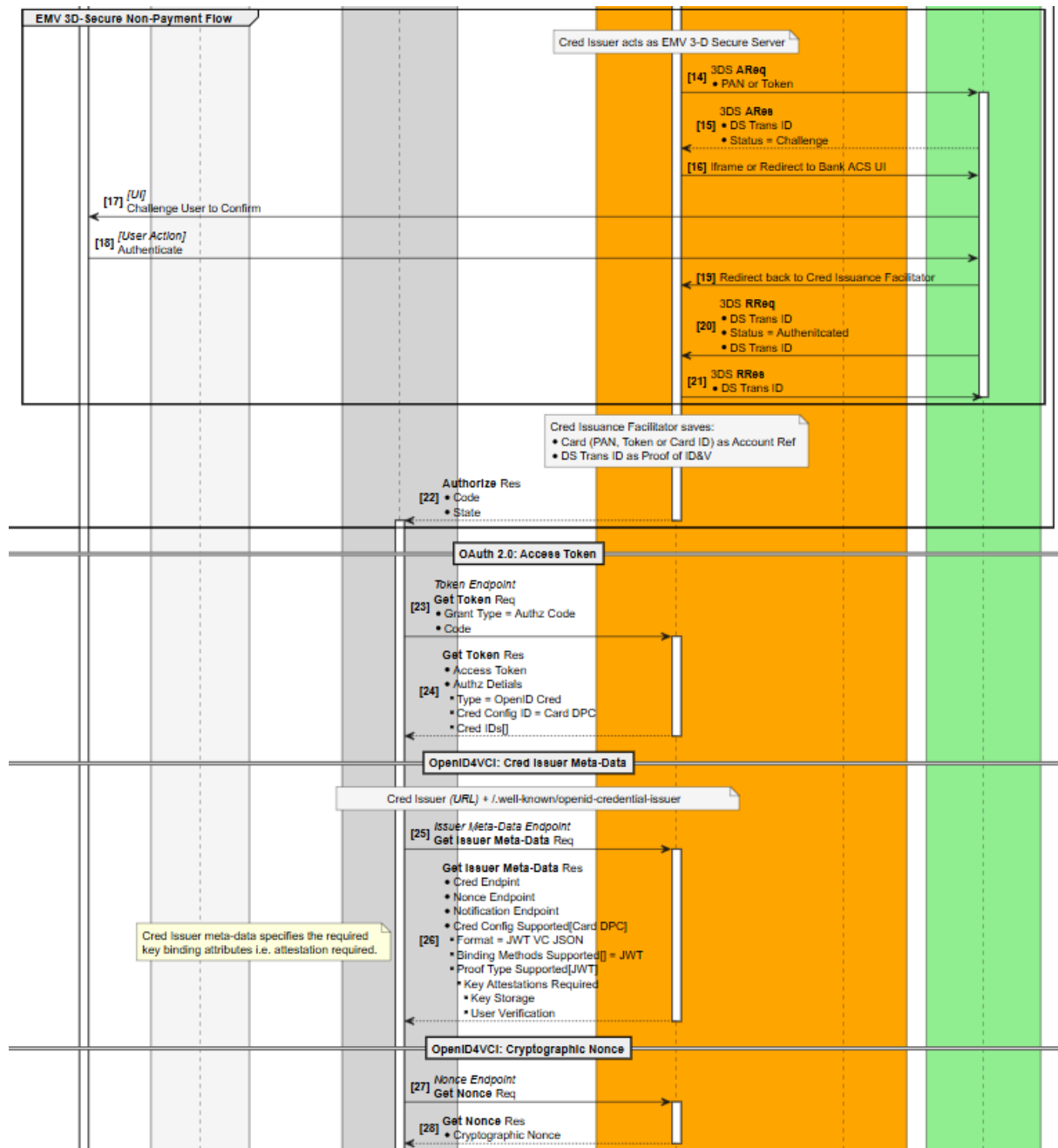


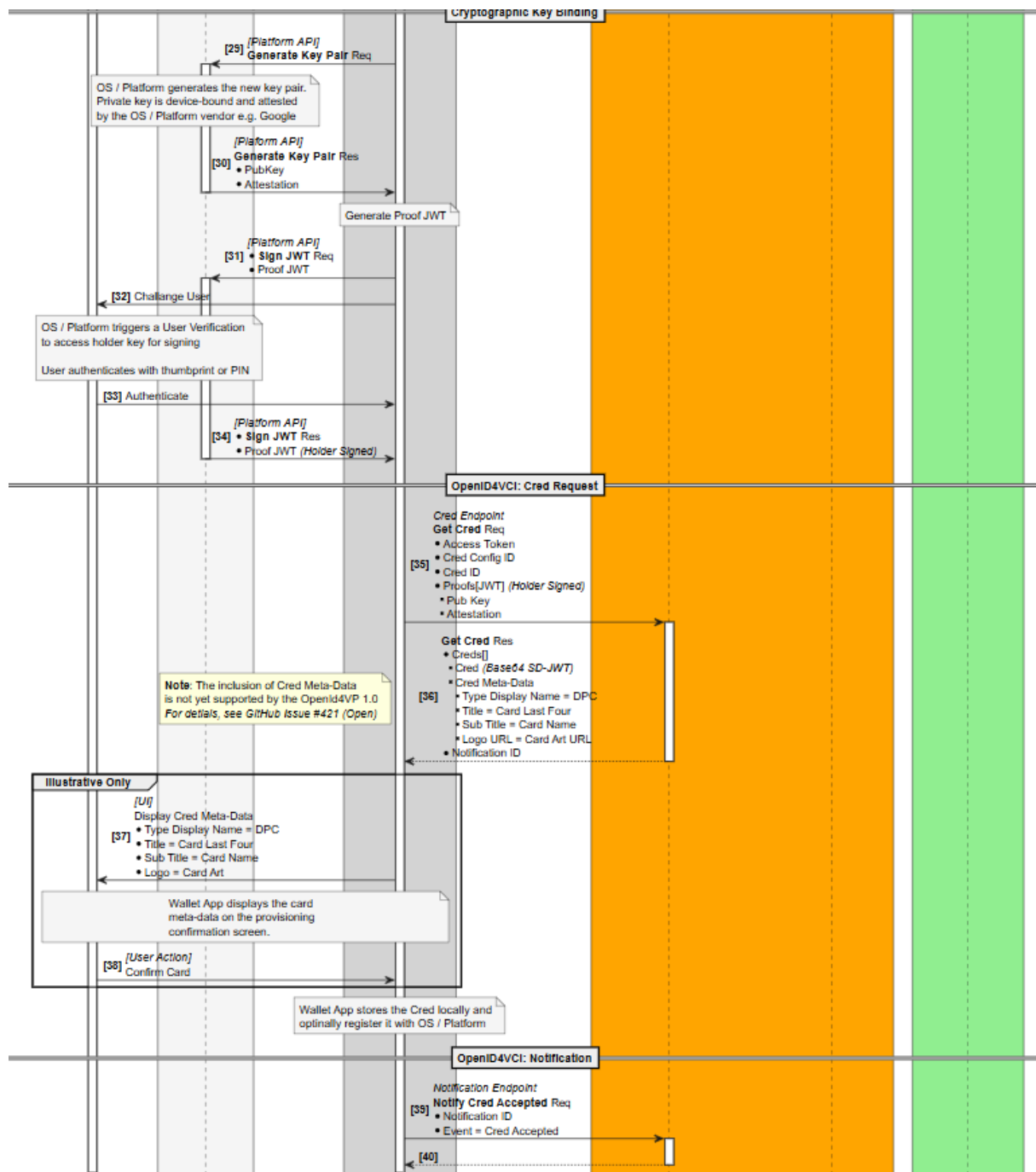




SD1 (B): MVP Flow 1: Provisioning of DPC through EUDIW directly integrated with card network (EAA provider)

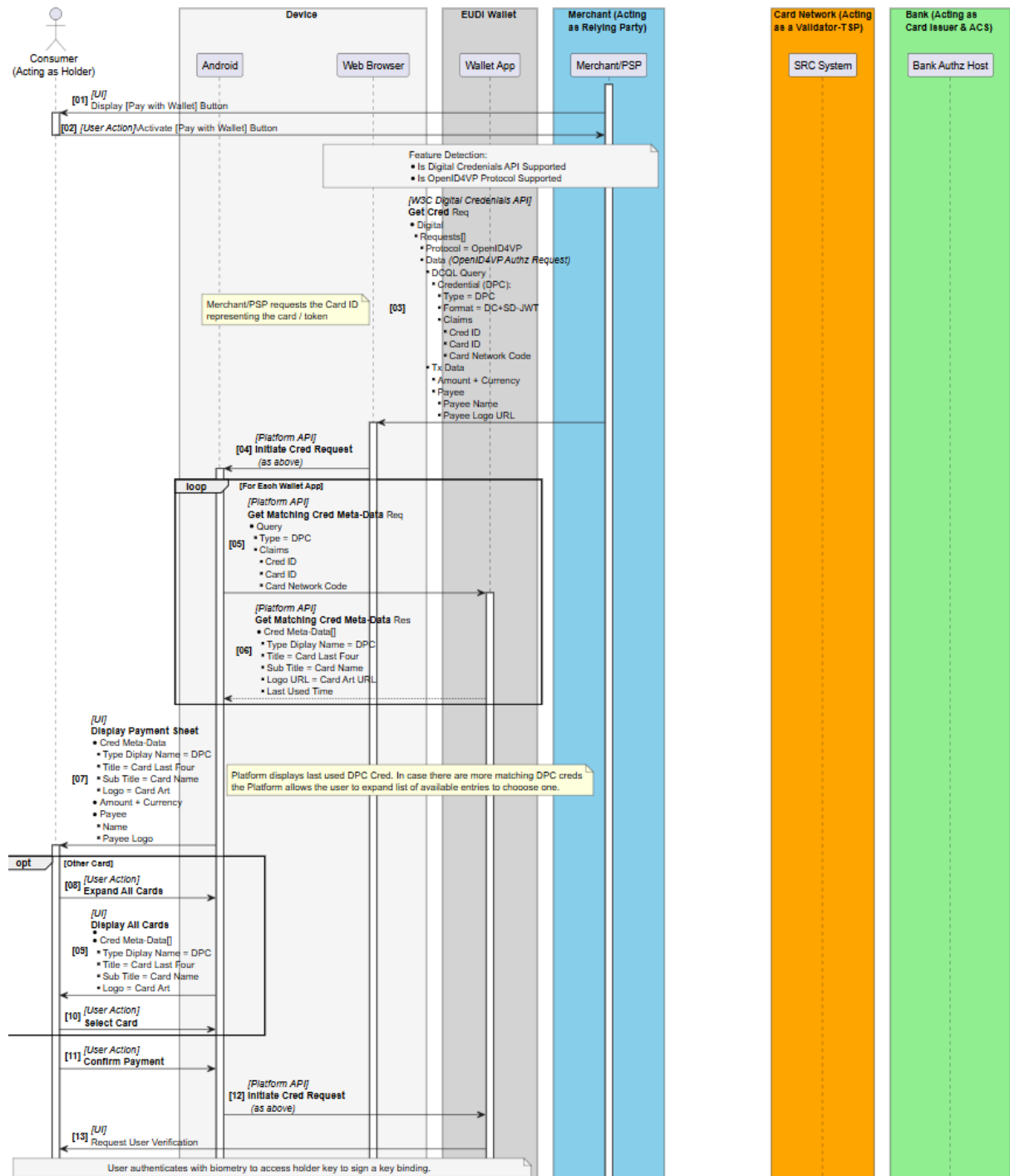


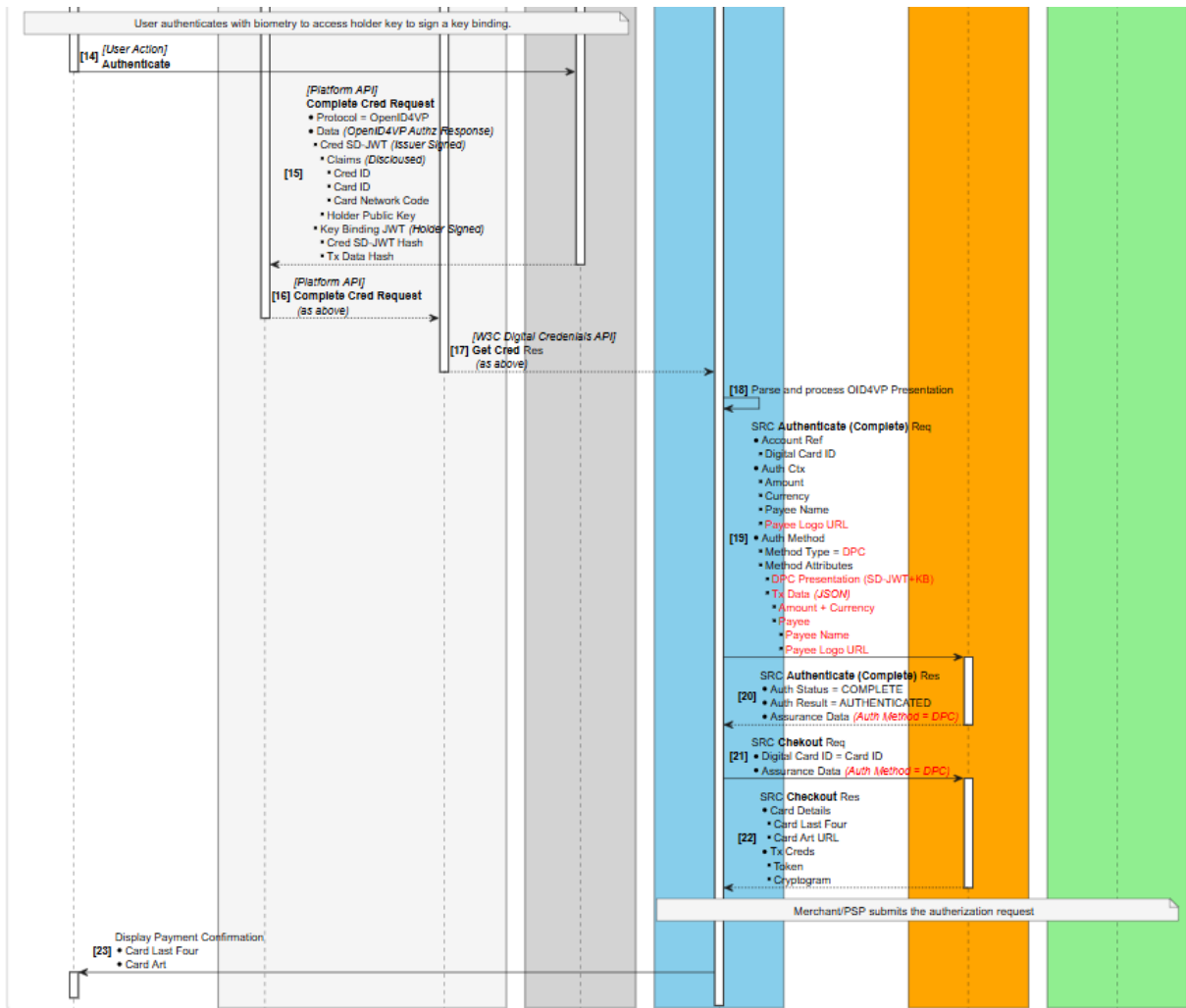




SD 2: MVP Flow 2: Presentation of DPC- Payment Initiation (Guest Checkout) using EUDIW

WE BUILD: WP3/PA2/B.2 - Presentation - Authenticated Guest Checkout

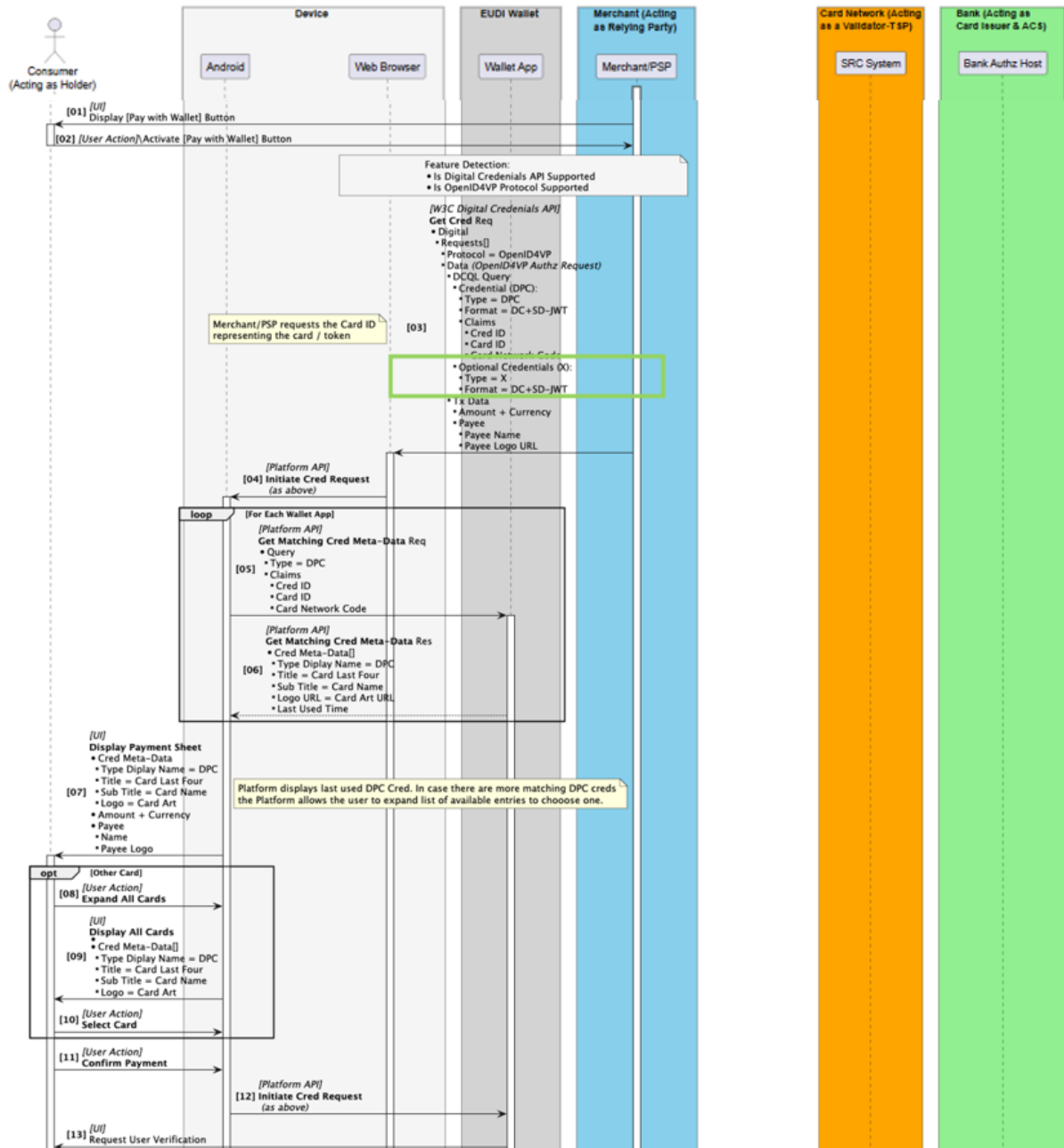


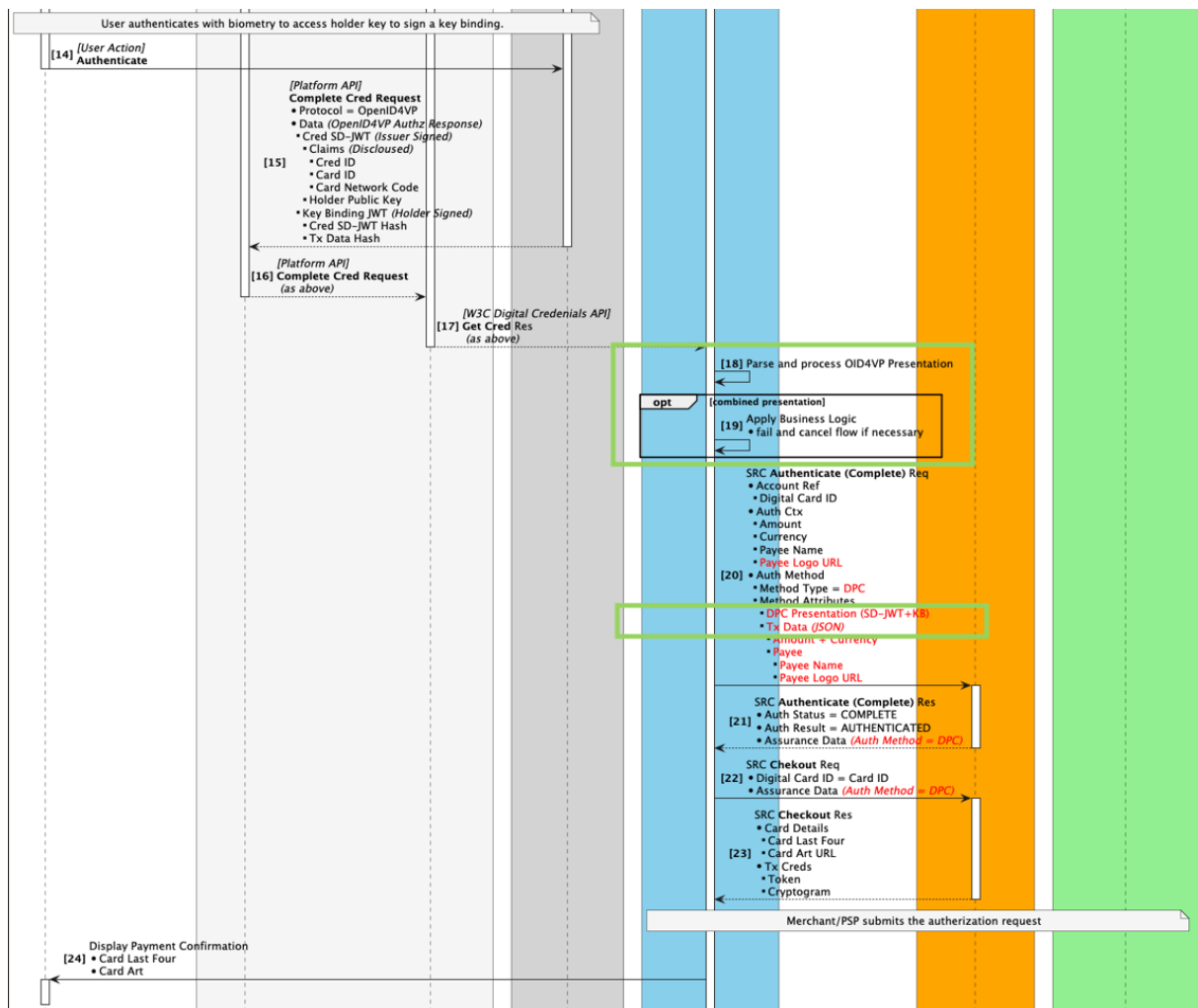


SD 3: MVP Flow 3: Presentation of DPC- Payment Initiation + Combined Presentation (Enhanced Guest Checkout)

This flow is same as MVP Flow 3 with following enhancements to include combined presentation:

- Step 3: Merchant requests DPC and ‘proof of eligibility’ credential as part of DCQL query
- Step 18: Merchant applies business logic to validate ‘proof of eligibility’ credential





WE BUILD consortium

Specification PA3

Scenario 1 –

Opening Bank Account

WP3 – Corporate Banking

Version : 1.0
Status :

final

Table of Contents

1 Introduction.....	3
1.1 <i>Objectives of this document.....</i>	3
1.1.1 Requirements Status by Project Phase	3
1.1.2 Most important open topics.....	3
1.1.3 Most relevant points for future revisions.....	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
2.2.1 MVP Restrictions	7
2.3 <i>Scenario main flow</i>	7
2.3.1 Legal Entity selection.....	9
2.3.2 Use Case specific additional data	10
2.3.3 Initiator identification	11
2.3.4 Legal entity identification & authorization	11
2.3.5 Initiator authorisation.....	12
2.3.6 UBO, Ownership & Control.....	13
2.3.7 Comparison of UBO information (issued by the QTSP over the transparency register)	13
2.3.8 UBO Verification.....	14
2.3.9 Summary of cross check & transfer in the internal system	14
2.4 <i>Scenario additional flows.....</i>	15
2.5 <i>Challenges and barriers.....</i>	15
2.6 <i>Working Assumptions.....</i>	16
3 Detailed scenario flow	17
4 Roles and participants	20
4.1 <i>Scenario roles and participants</i>	20
4.2 <i>Additional roles and partners.....</i>	20
4.3 <i>Target country combinations</i>	21
5 Attestations	22
5.1 <i>Introduction.....</i>	22
5.2 <i>Attestations to be provided by Authentic sources, other than the company</i>	22
5.3 <i>Created attestations in the scenario by the company's EBW</i>	22

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 1, as part of use case PA3 in work package 3 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	see MVP+ specification document	

1.1.2 Most important open topics

Date	Topic (Page)	Proposed	Solution
2026-05-27	VAT Rulebooks not available (#2.2.Scenario pre-conditions outline)	BU3 (VAT)	Document expected in July
2026-05-27	Tax Rulebooks not available (#2.2.Scenario pre-conditions outline)	PA1 (Tax)	Tax ID expected in July. Tax Nr- see the constraints specified in the 2.1 – Holder perspective

1.1.3 Most relevant points for future revisions

Topic	Description
Medium & Large Company Scope	We have agreed on a specific scope for the MVP. More advanced and realistic scenarios involving multiple owners, complex ownership and control structures (e.g., medium-sized and large companies) will be addressed as part of MVP+.
Liability transfer	The liability framework is transferred from the Issuer and Holder to the relying party (RP), since the MVP does not implement all verification steps defined in the target model of the MVP+. A detailed description of this individual verification steps is provided in Section 2.6. For the MVP, it has been agreed that certain verification activities will not be fully executed. Consequently, the RP assumes the associated liability and residual risk until the complete verification framework is implemented in future releases.

Topic	Description
	In MVP+, all verification steps are intended to be implemented and fully supported.

1.2 Scenario introduction

Scenario 1 (PA3) describes the cross-border onboarding of a registered EU company opening a business bank account in another EU Member State using the European Business Wallet (EBW) and the EUDI Wallet. The company may be a large enterprise, SME, or sole trader.

The scenario is designed to reflect one of the most complex real-world banking onboarding processes faced by financial institutions today. The onboarding of new business customers involves time-intensive screening activities and consumes significant operational resources at European banks.

With the Anti-Money-Laundering Regulation (AMLR, EU 2024/1624) coming into full effect in July 2027, harmonised European standards will replace fragmented national approaches, setting a new baseline for customer due diligence (KYC) across the EU. While AMLR defines what is required, eIDAS 2.0 and the upcoming European Business Wallet Regulation, provide the tools and the how to achieve it.

Therefore, in this scenario, the bank on-boards a new business customer in line with the upcoming AMLR data requirements, relying on trusted and verifiable attestations. The European Business Wallet (EBW) supports this process by acting as a key facilitator for regulatory compliance, operational efficiency, and legal certainty across national borders.

The scenario is based on the following documentation:

- **The WE BUILD Architecture & Integration Blueprint Reference document:** [D4.1 - Architecture & Integration Blueprint Reference Document v1.0 FINAL.pdf](#)
- **PA3 Stock Taking document:** <https://portal.webuildconsortium.eu/group/14/files/5922/collabora-online/view/3932>
- **PA3 Attestation requirements:** <https://portal.webuildconsortium.eu/group/14/files/6698/collabora-online/edit/4072>
- **AMLR:** <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1624>
- **Submitting beneficial ownership information** https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14851-Anti-money-laundering-formats-for-the-submission-of-beneficial-ownership-information-to-central-registers_en
- **Regulatory Technical Standards (RTS) under Regulation (EU) 2024/1624** https://www.aml.europa.eu/document/download/4ee33b25-2f03-4ed1-938b-a4ca36714d55_en?filename=Consultation%20paper%20RTS%20under%20Articles%2016%284%29%20and%2017%20of%20Regulation%20EU%202024162.pdf
- **Business Wallet Regulation:** <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0838>

- **ARF:** <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework>

2 Scenario specification

2.1 Introduction

Scenario 1 (PA3) covers the onboarding of a new banking client, a registered company in Country A, that wished to open a business bank account in another EU Member State (Country B) using the European Business Wallet (EBW).

The initiator¹ in country A holds an EUDI Wallet. Furthermore, user identification and verification of relevant UBOs are performed using the PID stored in their EUDI Wallets.

The designed MVP flow is based on BU1, and is the basis for subsequent flows following PA3 Scenario 1. The MVP process (Scenario 1-3) is executed sequentially by one natural person, the process ends with the triggering and issuance of the IBAN-OV issuance/attestation as EAA (means no additional onboarding is required).

The MVP, implemented in this scenario, covers:

For a Company

- The person initiating the account opening, simultaneously acts as **legal representative named in the EUCC²** and **ultimate beneficial owner (UBO)** for the bank.
- The scenario therefore represents a **one-person company structure** (e.g. a one-person *GmbH* in Germany), covering typical **SME use cases and also sole traders**. For large corporates running the MVP, we take in consideration only the company and not the entire relation with other legal entities. In case of relation with other legal entities (child or parent) this is supported within the MVP+ and will be specified there.
- The company is a **stand-alone legal entity** and is not in any relation with other legal entities
- The customer is non-CRS/FATCA relevant
- As a result, the initiator will be the **only person in the contact person and authorized signatories** shared with the bank.
- Basis for identification of initiator will be the PID held in an EUDI Wallet, verification of the UBO will also be done with the PID held in an EUDI Wallet. In practice, the natural person can choose how they want to identify themselves according to the declared identification means specified in the registry. We will present different variations in the MVP+.

For a Bank

- The company who wants to open a bank account will be classified as low/medium risk client. It will be no high-risk client. Internal bank processes (e.g.: sanction screening or PEP screening) will not consider in the MVP.

¹“Initiator” is a use-case-specific term referring to the person who initiates the bank account opening process. It is not a legal or regulatory term.

²Since the initiator and UBO is a primary legal representative as well in this specific case, no PoA is needed in the MVP flow. This will be covered and specified as part of the MVP+.

- The onboarding process will support companies with a LEI or VAT, since the required 3rd option: Tax, cannot be delivered until the delivery date of this document.
- The bank supports cross-border account opening without the need of registration in the national register for the initiator/account holder. If additional banks from countries that require an entry in the national register want to participate in the MVP, the need to include an additional POR needs to be revised. This is currently not in scope.

2.2 Scenario pre-conditions

To ensure the successful execution of this scenario, all of the following preconditions must be met:

- **EUDI Wallet with a PID:** The initiator and the relevant UBO must have access to an active and operational EUDI Wallet (e.g. holding a valid Wallet Unit Attestation, WUA). The EUDI Wallet contains Person Identification Data (PID) issued by a trusted PID issuer, enabling reliable identification and verification of the natural person as part of this use case. For further / up to date information please refer to [[GitHub: PA3: README: Authorised Person](#)].
- **EU Business Wallet with an EBWOID:** 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. For further / up to date information please refer to [[GitHub: PA3: README: Holder Business Wallet](#)]
- **Additional availability of Specific Digital Attestations in the EBW:** The business must have successfully requested and stored the following credentials within their wallet by undergoing the BU1 flow:
 - EUCC
 - VAT
 - Tax ID (for sole traders only)
 - Company Info
 - Contact Person

Furthermore, attestations will be issued as part of the PA3 flow:

- Ownership List
- Control List
- UBO List
- UBO List (by QTSP e.g. Bundesanzeiger)

- **A banking landing page (portal) is provided by the participating banks:** The initiator requests to open a bank account on a mocked banking website and starts the flow.
- **Harmonised trust infrastructure for attestation verification and issuance:** In order to trust the validity and authenticity of attestations (PID, QEAA, PubEAA and EAA) as defined in the MVP scope, a WE BUILD trust infrastructure is needed. This shall allow the Relying Party to validate the authenticity and integrity of the data provided by and to the Business Wallet(s). Furthermore, it needs to be assured that the issuer is listed as trusted on the respective trust list (PID issuer, EAA issuer, QEAA Issuer, etc.) and the needed Wallet Relying Party certificates (both for issuer and verifier) are held and valid. On the other side, the EUDI and EBW wallets need to consume and process this trust data and accordingly reflect if a trust aspect is not met (depending on the implementation this can be for example an alert or red cross) to notify the user.

2.2.1 MVP restrictions

- **Reduced Verification & Trust Reliance:** Neither seller nor buyer wallets perform full verification of attestation issuers, wallet integrity, or attestation binding as it is envisioned in the MVP+.
If EAA providers are included in the WE BUILD specific trust lists (LOTL trust infrastructure) and Wallet Providers support these lists, then EAA issuer verification can be demonstrated. However, this approach is primarily suited to the WE BUILD context and may not extend beyond the project context. The member states have indicated that, due to scalability reasons, only QTSPs will be included in a production TLOL. Therefore, the WE BUILD-specific TLOL serves merely as a showcase and is not applicable outside of the consortia.
Implication: The system relies on assumed trust rather than the level of cryptographic validation envisioned for the MVP+. For high-assurance scenarios, dealing with EAAs, this would impose a high risk if rolled-out as is to production.
- **Relying parties using a verifier component vs. a complete European Business Wallet:** A key question that was identified is whether banks (as relying parties) can leverage their existing verifier components in alignment with the EUDI Wallet, or whether they would also need to introduce holder/wallet capabilities. Feedback from participating banks indicates a strong preference for reusing existing infrastructure. At the same time, companies have emphasised that, for assurance purposes, they would expect an initial exchange of attestations—such as EBWOID and EUCC—before sharing sensitive data with a bank.
Implication: In this use case, the exchange of these attestations is demonstrated as a manual process (automation with relevant trust aspects will be covered in MVP+ and is specified there).
- **The RP does not share a Wallet Unit Attestation (WUA) during verification:** A company interacting with a Relying Party would like to also check wallet unit attestations of the RP European Business Wallet. This is based on the current WE BUILD draft not foreseen. However this would be an important feature for holders for securely identifying the relying party.

Implication: Advanced peer-to-peer identification and consent workflows allowing holders to check the verifiers wallet unit attestations are not yet supported in this MVP.

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

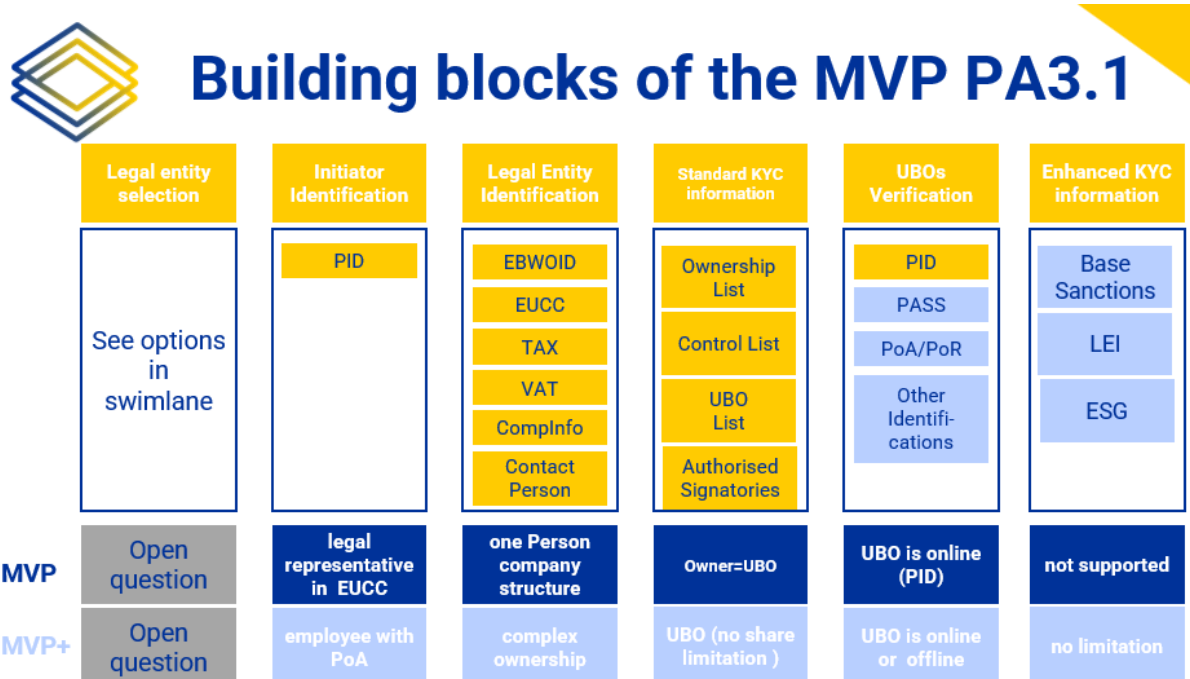
Implication: Limits handling of complex risk scenarios and data consistency.

- **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.

2.3 Scenario main flow

The main flow represents an end-to-end cross-border onboarding process.. It shows the interaction between the potential customer, natural and legal person's wallet(s), issuers, and the bank as relying party.



Process Overview

Attached is a high-level overview of the building blocks.

The order of these blocks can be defined by the party operating the MVP. The MVP also provides the flexibility to activate or deactivate individual building blocks, allowing only the required parts of the flow to be executed.

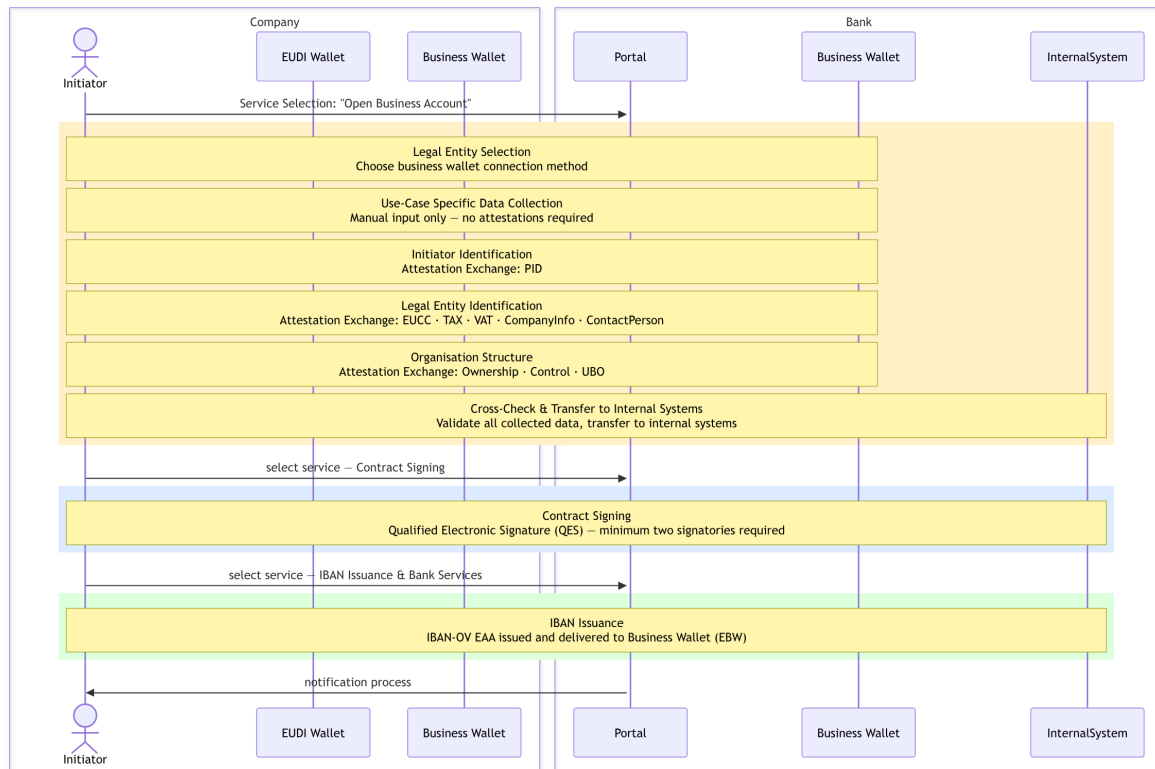


Figure 1: Workflow Overview ([add link](#))

Prerequisite: Attached is also an overview of the prerequisites for the Holder and the Verifier required to run the use case.

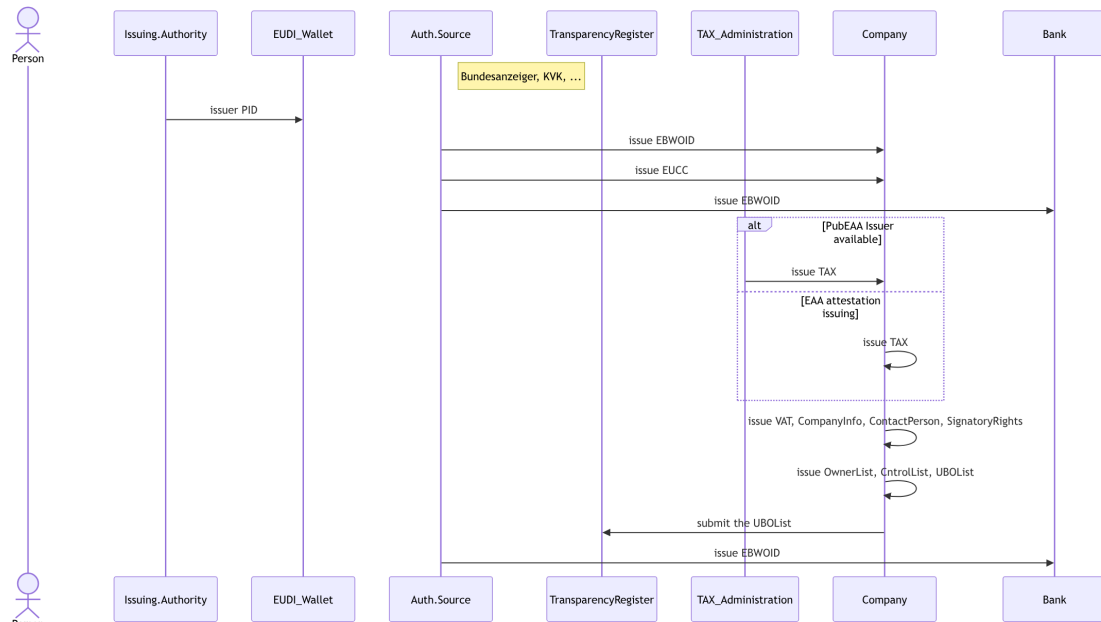


Figure 2: [Prerequisites](#)

Holder (EUBW) pre-requisites (see the RP requirements specified in the 360Degree Document file).

- EBWID: Issued by an authorized source (PubEAA or QEAA).
- EUCC: Issued by a QTSP (QEAA).
- Tax Information: Issued by the Tax Administration (QEAA) or provided by the initiator.
- VAT Information: Issued by the Tax Administration (QEAA) or by the company (EAA).

2.3.2 Use case specific additional data

The following additional information are need it to be manually specified per request for a complete KYC flow (as input):

1. Expected turnover / activity volume
2. Purpose & intended nature of business relationship

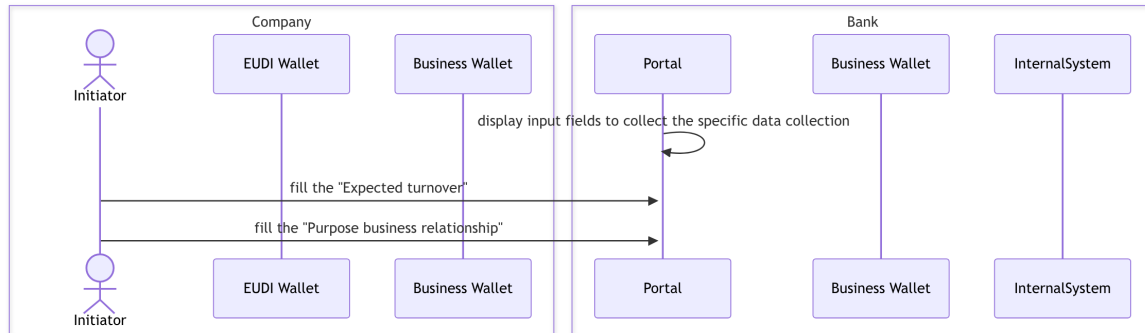


Figure 4: UC Specific Data Collection (add link)

2.3.3 Initiator identification

The person initiating the account opening process is a legal representative of the company using the PID held in the EUDI Wallet to identify.

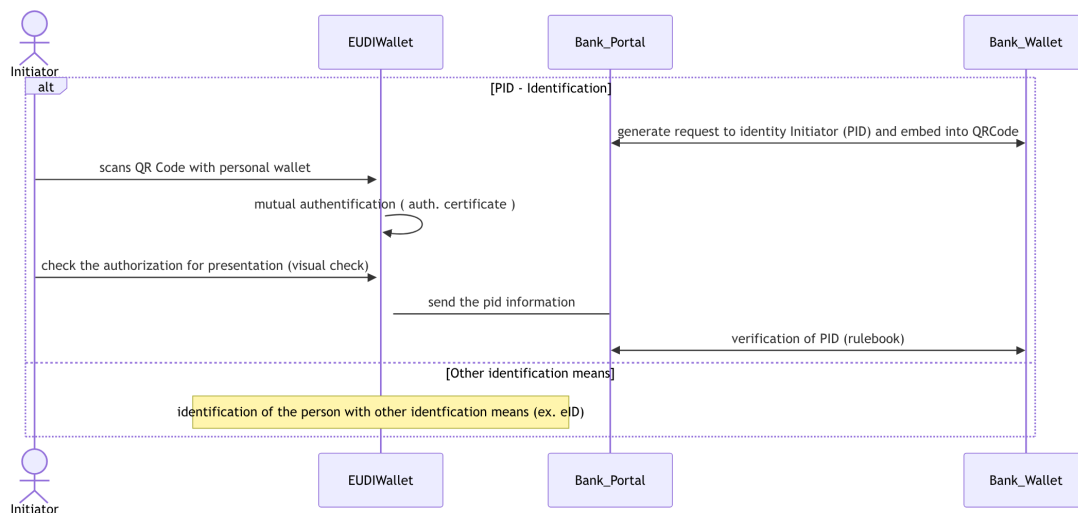


Figure 5: [Initiator Identification](#)

2.3.4 Legal entity identification & authorization

The following attestations are verified (i.e. integrity check):

- EBWOID
- EUCC

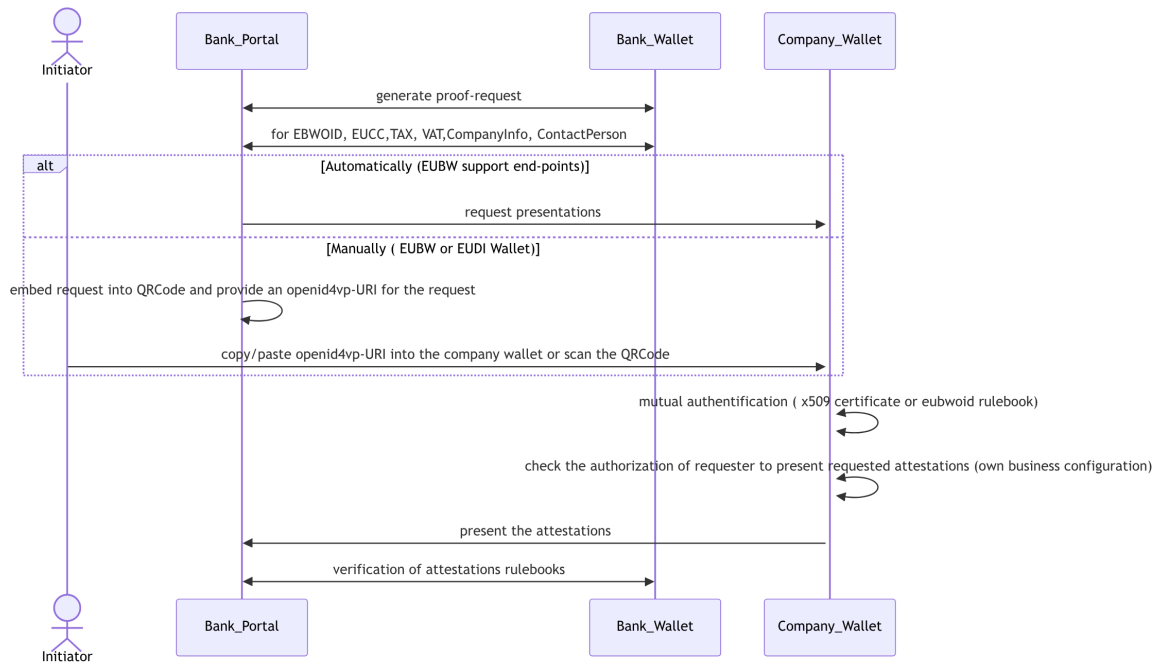


Figure 6: [Legal Entity Base Identification](#)

2.3.5 Initiator authorisation

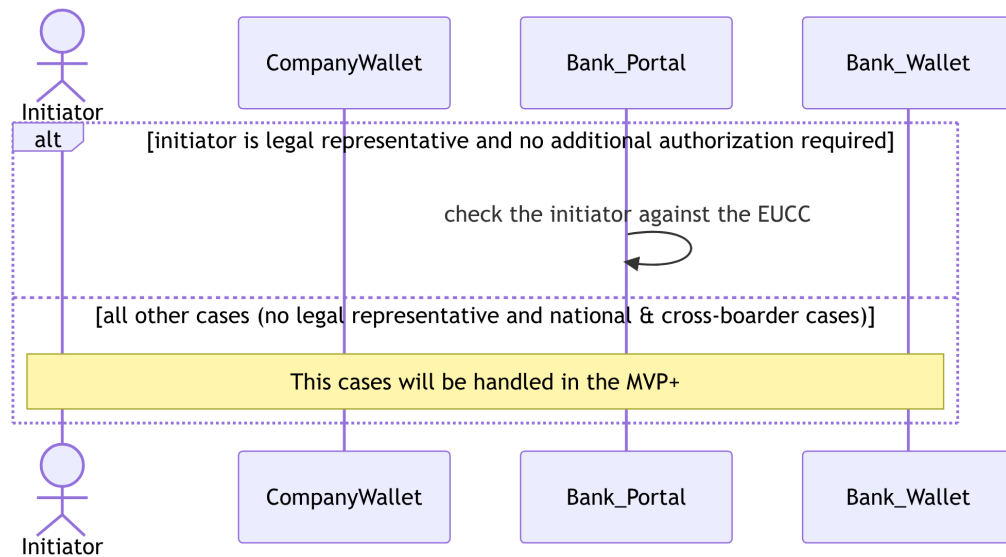


Figure 7: [Initiator Authorization](#)

The bank verifies whether the initiator is listed in the EUCC1 as the legal representative. If this condition is met, the process continues; otherwise, it is stopped, and the use of MVP+ is recommended.

The bank also verifies whether the EUCC covers only a sole-proprietor or one-person company scenario, with no relationships to other legal entities. If this condition is met, the process continues; otherwise, it is stopped, and the use of MVP+ is recommended.

Additional data gets automatically requested:

- VAT
- Tax ID (for sole traders only)

- Company info
- Contact person

2.3.6 UBO, Ownership & Control

In this step the UBO, ownership, and control list held by the company is verified by the bank.

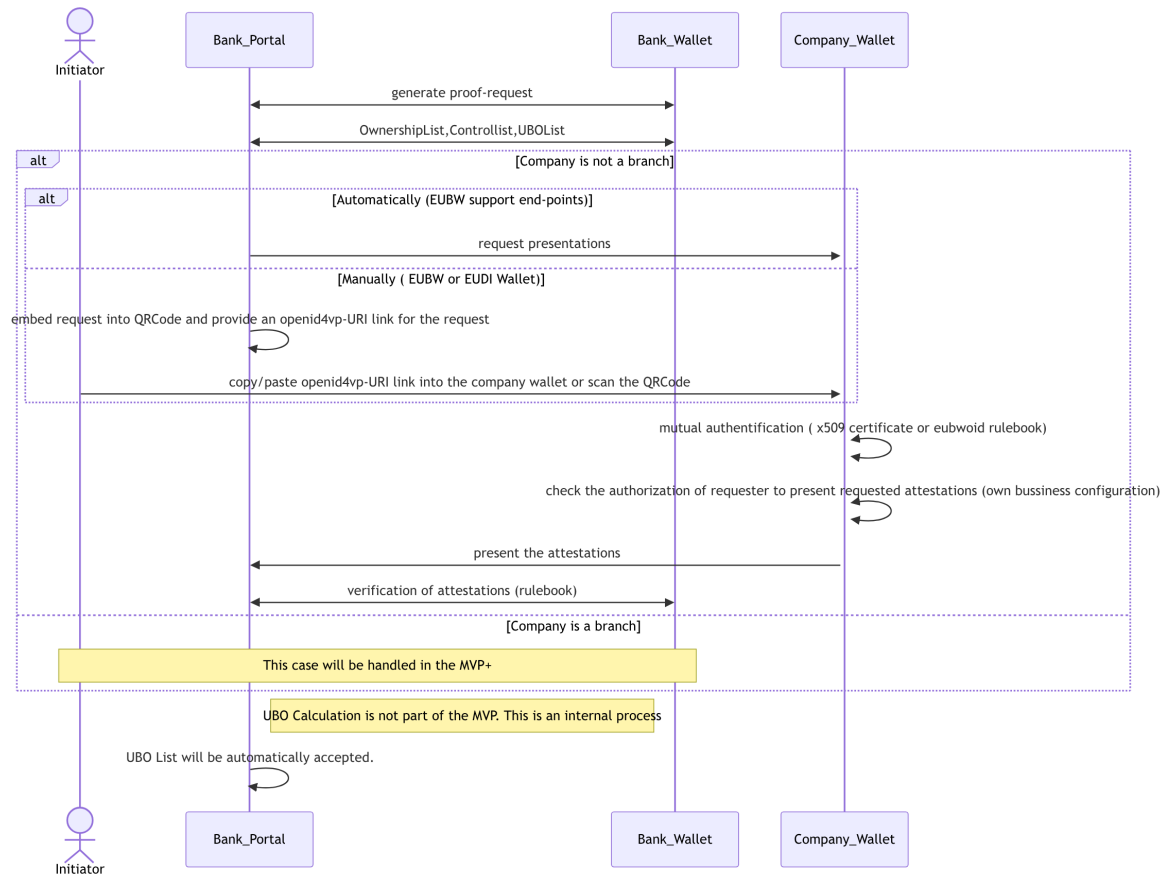


Figure 8: [Ownership & Control Structure Information](#)

2.3.7 Comparison of UBO information (issued by the QTSP over the transparency register)

For the account opening process, banks require: the UBO list issued by the client and a UBO list issued by a QTSP over the transparency register. On the basis of the clients delivered UBO list, the bank will do their own UBO calculation. In the MVP, the banks own calculation and the two received UBO list attestations presented contain consistent and coherent information. Therefore no discrepancy report to the register necessary.

Furthermore, UBO calculation is a bank internal process and is not part of the MVP nor MVP+.

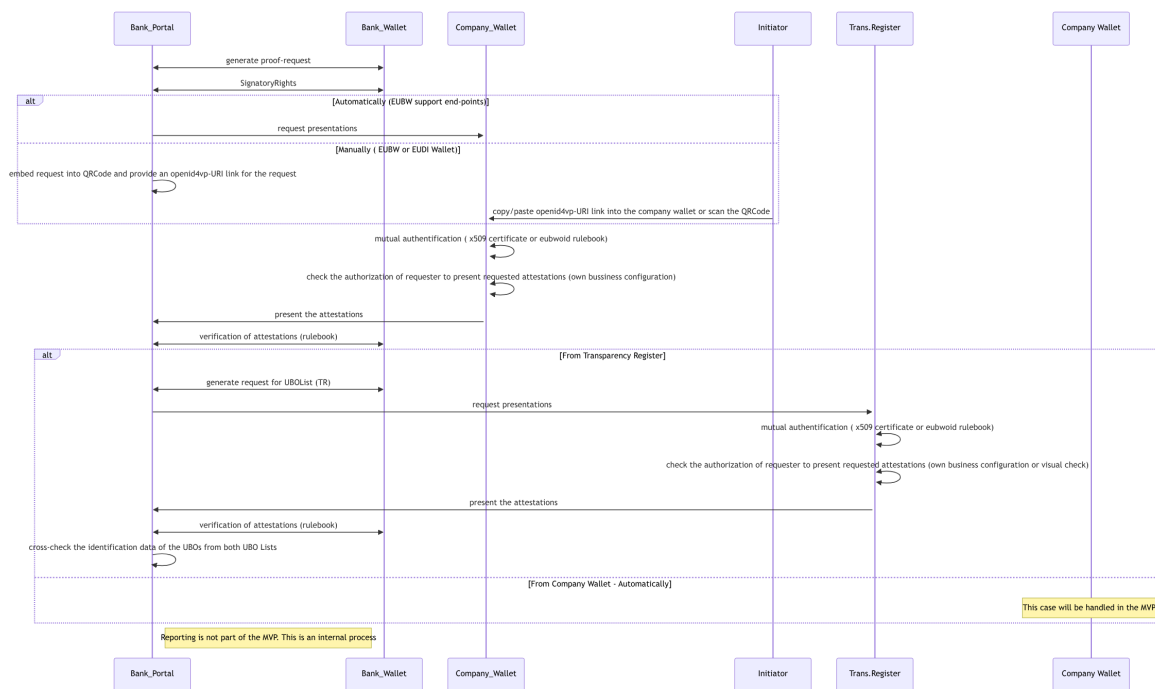


Figure 9: Signatory Rights & UBO List from Transparency Register

2.3.8 UBO verification

After a successful comparison of the UBO lists, the UBO's are verified. For the MVP, this is being done by the bank using the online verification process with the PID of the UBO.

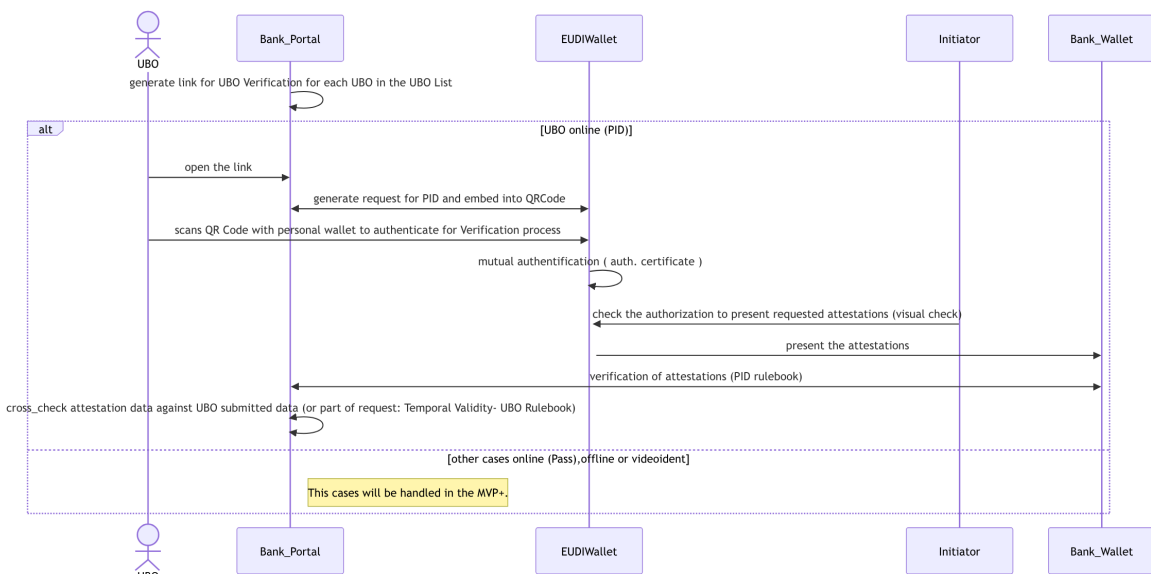


Figure 10: UBO Verification

2.3.9 Summary of cross check & transfer in the internal system

After the bank obtained all the necessary information, a cross-check of all these information and the internal bank systems is being done. A summary of the cross-check will be presented in the bank's portal. Finally, the bank transfers the information into its internal system.

For the MVP there will be no live integration of the bank internal system.

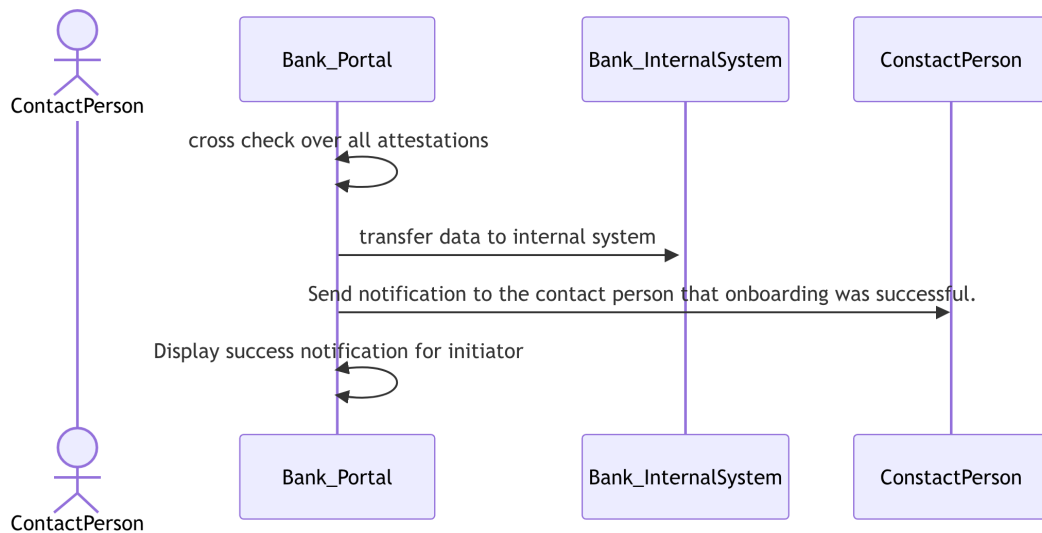


Figure 11: [Cross Check](#)

Note: Contact Person = Initiator !

2.4 Scenario additional flows

No additional flows are designed as part of this scenario,

2.5 Challenges and barriers

As outlined in the specification document section 1.1.5, this use case is based on a set of assumptions that allow coverage of most relevant scenarios taking simplification assumptions. However, special or edge cases would need to be revisited and addressed when designing a production-grade implementation.

This is covered in the MVP:

- manual 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>

Description	Process
4.2.1 Verification of the cryptographic integrity and signature validity of the attestation.	MVP Scope
4.2.2 Verification of the authenticity of the received attestation ("genuinity" check)	MVP Scope: only if the WE BUILD TLOL integration and the functionality is supported by the Wallet Provider;

Description	Process
4.2.3 Verification of the issuer's identity	MVP Scope: only if the WE BUILD TLOL integration is available and the functionality is supported by the Wallet Provider; MVP Out-of-Scope: Historical trust validation (e.g., validation across updates, certificate renewals, or key rollovers) is out of scope for the MVP and will be addressed in MVP+
4.2.4 Verification that the issuer is authorized to issue the attestation and that the issuer is accepted according to verifiers policies	MVP Scope PubEAA and QEAA: if the WE BUILD TLOL integration is available, without historical trust validation, and the functionality is supported by the Wallet Provider EAA: Supported if the WE BUILD TLOL integration and Wallet Provider capabilities are available. MVP Out-of-Scope Historical trust validation (e.g., validation across updates, certificate renewals, or key rollovers) is out of scope for the MVP and will be addressed in MVP+. Chaining: Recursive trust-chain validation (chaining) shall be demoed in the MVP+ - discussions are ongoing and no decision will be available or timely implemented for the MVP.
4.2.5 Verification of validity periods, expiration, and issuance timestamps.	MVP Scope: only if Wallet Provider capabilities are available;
4.2.6 Verification that the attestation has not been revoked or suspended.	MVP Scope: only if Wallet Provider capabilities are available;
4.2.7 Verification of the wallet integrity by verifying the wallet unit attestation	MVP Scope: only for EBW and if Wallet Provider capabilities are available;
4.2.8 Verification that the attestation is cryptographically bound to the holder's wallet instance.	MVP Scope: only for EBW and if Wallet Provider capabilities are available;

Further key challenges that this use case highlights include the need for clear decisions and/or technical specifications in the MVP+:

- Wallet discovery mechanisms (endpoint retrieval – see screenshot 2.3.1), there is an ADR pending. The use case parties can incorporate this, if relevant to them. Alternatively they can use other options outlined in 2.3.1
- Automation capabilities related to the EBW

2.6 Working assumptions

See section 2.2 Scenario pre-conditions.

Further, the company in automated flows is authorised to present attestations and receive attestations (no configuration support).

3 Detailed scenario flow

Main flow step – same-device web-site to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Legal Entity selection & Business Flow	Initiator (representing the Company)	Initiator (natural person) accesses the bank (or WE BUILD generic) landing page and selects the service “Open a business bank account”.	Onboarding landing page remains an open topic. Company holds an active EBW with valid EBWOID.	
	Bank	Bank initiates and proceeds with the opening a bank account flow		
Initiator identification via PID	Bank	Bank displays QR code and requests PID attributes required for identification of the initiator.	Bank registered as Relying Party.	
	Initiator	Presents PID data from EUDI Wallet	Initiator holds an active EUDI Wallet with valid PID.	
	Bank	PID data is verified by the bank.		
Additional data provisioning	Initiator	Initiator enters the two mandatory attributes.		
Legal Entity Identification	Bank	Bank requests company-related attestations from the company’s EBW.		
	Company	The company presents the following attestations: • EBWOID • EUCC	EBW holds the valid attestations.	

Main flow step – same-device web-site to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
	Bank	The Bank verifies the attestations. The Bank checks that the initiator is a legal representative named in the EUCC.	Consistency between PID and EUCC data.	
	Company Wallet	The following data is requested automatically by the bank, based on the prior authorization of the initiator and the EUCC. • VAT • Company Information • Contact Person		• Tax ID (for sole traders)
Verification of additional financial KYC information	Bank	Bank requests and verifies: • Ownership List • Control List • UBO List (company-issued)		Not relevant for sole traders
	Company (EBW)	Company shares the relevant attestations	EBW holds the company-issued attestations.	If not yet held in the EBW, then the company must issue them to the EBW.
	Bank	Bank request the UBO List from transparency register.		
	Bank	Bank compares UBO list provided by the company with UBO list from transparency register. Confirms consistency between both UBO sources.		

Main flow step - same-device web-site to app	Actor	Interpretation or reference	Dependencies	Variations and exceptions
Cross-check and review of summary	Bank	Bank performs internal checks using a summary view of verified attestations and notifies the initiator about the successful onboarding.		

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Countries
1. User of Wallet	Bosch	DE, NL
	Infocert	IT
	SBB	CH
	VOEST ALPINE	AT
	DB-CARGO	DE
2. Authentic Sources (public registry)	Bundesanzeiger	DE & other European countries
	Infocamere	IT
	KVK & NL Tax agency	NL
	Ministry of development	PL
3. Relying Party (=Bank)	Deutsche Bank	DE
	Czech Banks (currently being onboarded)	CZ
	Banca Sella	IT
	Pekao SA	PL
	ABN AMRO (final confirmation pending)	NL
	RBI	AT
4. Intermediary	Infocert (act as tech provider for BancaSella)	IT
	BankID (Act as Techprovider; scope to be confirmed)	CZ
	Doxallia (act as tech provider for Banc Agricole)	FR
	PWPW (act as tech provider for Pekao SA)	PL

Authentic sources in this use case are needed for companies and financial institutions (RP). The RP require for the MVP flow an EBWOID and EUCC, therefore less data requirements arise for authentic sources covering this.

We have created a more comprehensive overview:

<https://portal.webuildconsortium.eu/group/14/files/9105/collabora-online/read/4534>. Since this document is subject to change please refer to Appendix 2: PA3 MVP Partner Overview for an overview as of 2026-06-22.

4.2 Additional roles and partners

Primary role	UC partner Name	Countries	Wallet
1. EUDI Wallet provider	Digidentity B.V.	all	NP
	Procivis	all	NP
	Governikus	D	NP
	SWIYU (Swiss Reference Implementation)	CH	NP
	Aricoma	CZ	NP
2. EBW Provider	Spherity	DE	LP
	Procivis	AT	LP
3. PID Provider	Governikus	DE	NP
	Infocamere	IT	NP
	Aricoma	CZ	NP
4. Trusted list registrar	Following the Trust List Group	na	na

Primary role	UC partner Name	Countries	Wallet
5. QEAA provider	Digidentity B.V.	all	All
	Procivis in collaboration with QTSPs	all	All
6. Pub-EAA provider	Na	Na	Na
7. EAA provider	Any company of 4.1 section 1, given we need self-issued attestations in the use case	See above	See above
8. QES provider	Digidentity B.V.	all	All
	Procivis in collaboration with QTSP	all	All

4.3 Target country combinations (MVP)

Partners over-view ¹		Relying Party Country (Bank)							
		AT	NL	DE	IT	CZ	CH	FR	PL
Holder Country	AT								
	NL			x					
	DE								
	IT				x				
	CZ								
	CH								
	FR								
	PL								

Current working assumption is that we achieve conformance within the use case. And that any wallet provided within the country can be used across borders.

¹Final confirmed constellations only; however most countries indicated that participating in MVP/MVP+ may be confirmed at a later stage.

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.

Overview over the attestations and required attribute, in line with AMLR requirements: [360° Attestation Requirements Collection](#). In addition to that you can please find the excerpt list of the attestation requirements for the MVP implementation in

5.2 Attestations to be provided by authentic sources/QTSP/EAA, other than the company

Attestation name	Short description	To be provided by	Requirements
EBWID	Annex 1	Auth,Source	
EUCC	Annex 1	Auth,Source	
Tax ID	Annex 1	Auth,Source	
VAT	Annex 1	EAA - Attestation	
UBO List	Annex 1	QTSP	
Company Info		QEAA	

5.3 Created attestations in the scenario by the company's EBW

EAA – Attestation issued by the company out of the Business Wallet

Attestation name	Short description	Applicable domain standards
Company Info		EAA - Attestation
Contact Person		EAA - Attestation
Ownership List		EAA - Attestation
Control List		EAA - Attestation
UBO List		EAA - Attestation
Authorised Signatories		EAA – Attestation

Annex 1 – 360° attestation requirements – MVP except

Attestation Scheme	Data Point	Description	Required by	Regulation
-no scheme required-	Expected turnover / activity volume	see Data Point	EU-AMLR 2027ff	RTS §34
-no scheme required-	List of operating countries	ISO Codes of Countries where the company has a business activity - needed because for opening a bank account a preliminary risk assessment needs to be done (e.g not operates in Russia). Should include all countries (not e.g top 10 only).	Other (please comment)	Bank Internal Req.
-no scheme required-	Purpose & intended nature of business relationship	see Data Point	EU-AMLR 2027ff	Art. 24 AMLR
CIU	CIU	Collective Investment Undertaker: Distribution (Fund clients) – Identification of final investor	EU-AMLR 2027ff	Art. 23 RTS
CompanyInfo	Full legal name (1st history)	the complete historical legal name if available	EU-AMLR 2027ff	Art. 2, 22(1)(a)-(d) AMLR
CompanyInfo	Full legal name (2nd history)	the second historical legal name if available	EU-AMLR 2027ff	Art. 2, 22(1)(a)-(d) AMLR
CompanyInfo	Number of employees	The number of the employee of the legal entity	Other (please comment)	Bank Internal Req.
CompanyInfo	Source of Funds (SoF)	see Data Point	EU-AMLR 2027ff	Art. 24, 34 AMLR
CompanyInfo	Trade/alias name	the auxiliary historical legal name if available	EU-AMLR 2027ff	Art. 2, 22(1)(a)-(d) AMLR
ContactPerson	Email	The bank may want to recontact the company or the individual opening the bank account, for problem solving or other questions	Other (please comment)	Bank Internal Req.
ContactPerson	Full name	The bank may want to recontact the company or the individual opening the bank account, for problem solving or other questions	Other (please comment)	Bank Internal Req.

Attestation Scheme	Data Point	Description	Required by	Regulation
ContactPerson	Telephone number	The bank may want to recontact the company or the individual opening the bank account, for problem solving or other questions	Other (please comment)	Bank Internal Req.
Control List	Citizenship	The citizenship of natural person	EU-AMLR 2027ff	AMLR Art. 51+52
Control List	Control %	The percentage of control a legal or natural person exerts over another company.	EU-AMLR 2027ff	AMLR Art. 51+52
Control List	Full name	Fullname or legal person of the direct owner	EU-AMLR 2027ff	AMLR Art. 51+52
Control List	Legal name or EUID	Identification of the legal entity	EU-AMLR 2027ff	AMLR Art. 51+52
Control List	Location of Birth	The Location for the natural person	EU-AMLR 2027ff	AMLR Art. 51+52
ControlStructure	Controlstructure List	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+53
EDD	EDD	Reputation, family members or known close associates	EU-AMLR 2027ff	Art. 17 (RTS adapted from Art. 21 AMLR)
EU PoA	Authorisation scope for initiator	What is the delegate allow to do on behalf of the company? --> note that "initiator" = not considered a legal term. How we understand it: a legal representative or a person that has authorisation to initiate the relationship based on their role or take the action triggered.	Other (please comment)	Bank Internal Req.
EU PoA	Count Limitation	the count limitation	Other (please comment)	Bank Internal Req.
EU PoA	Financial Limitation	the financial limitation	Other (please comment)	Bank Internal Req.
EU PoA	name of initiator	Name of the delegate that holds the PoA / PoR --> note that "initiator" = not considered a legal term. How we understand it: a legal representative or a person that has authorisation to initiate the relationship based on their role or take the action triggered.	Other (please comment)	Bank Internal Req.
EU PoA	role of initiator	the role the of the person	Other (please comment)	Bank Internal Req.
EU PoA	Time Limitation	the time limitation	Other (please comment)	Bank Internal Req.
EUCC	Activity code (local/NACE)	activity code/description	EU-AMLR 2027ff	AMLR Art. 15; RTS §34

Attestation Scheme	Data Point	Description	Required by	Regulation
EUCC	Birth date of authorised representative	see Data Point	EU-AMLR 2027ff	Art. 23(2) AMLR
EUCC	Country of incorporation	Country of incorporation	EU-AMLR 2027ff	Art. 22(1)(b) AMLR
EUCC	Date of registration / incorporation	Date of registration / incorporation	EU-AMLR 2027ff	AMLR Art. 13(1)(a)
EUCC	Decision scope (sole decision maker or with another person) of authorised representative	Content (Values) of the data field needs to be harmonized across countries!	EU-AMLR 2027ff	Art. 23(2) AMLR
EUCC	Legal form (e.g., DE206)	legal_form_standard	EU-AMLR 2027ff	Art. 22(1)(b) AMLR
EUCC	Legal form (e.g., Ltd., GmbH)	legal form acronym	EU-AMLR 2027ff	Art. 22(1)(b) AMLR
EUCC	Legal form (e.g., Ltd., GmbH)	legal form description in english		
EUCC	Legal form description (ex. Gesellschaft mit beschränkter Haftung)	legal_form_description in the local language		
EUCC	List of legal representatives	Array listing the legal representatives of the company (fullname, birthdate, role and decision scope)	EU-AMLR 2027ff	Art. 23(2) AMLR
EUCC	Registered address (legal persons)	the registered address	EU-AMLR 2027ff	Art. 22(1)(b) AMLR
EUCC	Registered office address	the registered office		Cross-check via company registry or LEI where applicable

Attestation Scheme	Data Point	Description	Required by	Regulation
EUCC	Registered post address	the registered post (if available)		Art. 6 & 7 RTS define acceptable documents; must contain name, DOB, ID number, security features
EUCC	Role of authorised representative	Content (Values) of the data field needs to be harmonized across countries!	EU-AMLR 2027ff	Art. 23(2) AMLR
EUCC	Senior Managing Official (SMO) info	<to be explained in more detail>	EU-AMLR 2027ff	Art. 63(4) AMLR
IBAN Ownership Verification	Bank BIC	see Data Point	Other (please comment)	IBAN – Issuing process
IBAN Ownership Verification	Bank Name	see Data Point	Other (please comment)	IBAN – Issuing process
IBAN Ownership Verification	Holder name	see Data Point	Other (please comment)	IBAN – Issuing process
IBAN Ownership Verification	IBAN	see Data Point	Other (please comment)	IBAN – Issuing process
Initial Customer Risk Rating	Risk category assignment (prior to exemption / SDD)	individual action from banks in their back office. No general business wallet function	EU-AMLR 2027ff	Art. 19(7), 28 AMLR
Legal Entity Identifier	LEI – Legal Entity Identifier	LEI Identification	EU-AMLR 2027ff	Art. 22(1)(b), Recital 23 AMLR
LPID/EBWOID/OID	Company/trust registration number (EU-ID)	EUID number (according to the BRIS nomenclature)<CountryCode><Location>.<Registername><RegisterCode>	EU-AMLR 2027ff	Art. 22(1)(b) AMLR
LPID/EBWOID/OID	Full legal name	the official name according to the national register	EU-AMLR 2027ff	Art. 2, 22(1)(a)-(d) AMLR
Ownership list	Citizenship	This is needed already during opening a bank account to prove within 30D that person opening bank account is not US citizen	EU-AMLR 2027ff	AMLR Art. 51+52

Attestation Scheme	Data Point	Description	Required by	Regulation
Ownership list	Citizenship	This is needed already during opening a bank account to prove within 30D that person opening bank account is not US citizen	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership list	Full name	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership list	Full name	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership list	Legal name or EUID	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership list	Legal name or EUID	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership list	Location of Birth	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership list	Location of Birth	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership list	Ownership %	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership list	Ownership %	Additional infos, see PID	EU-AMLR 2027ff	AMLR Art. 51+52
Ownership-Structure	Ownership-Structure	Coexistence of ownership interest and control in the ownership structure	EU-AMLR 2027ff	AMLR Art 51+54
PEPPoID	PEP assessment	Client / UBO / SMO / acting persons	EU-AMLR 2027ff	Art. 34 AMLR
PEPPoID	PEP Status	pep_status	EU-AMLR 2027ff	AMLR Art. 20
PID	Date of birth	natural person can be UBOs or Initiator (legal repr, signatory rights, mandate person)	EU-AMLR 2027ff	AMLR Art. 13(1)(a)
PID	Full name (Natural Person)	natural person can be UBOs or Initiator (legal repr, signatory rights, mandate person)	EU-AMLR 2027ff	AMLR Art. 13(1)(a)
PID	Government-issued ID	natural person can be UBOs or Initiator (legal repr, signatory rights, mandate person)	EU-AMLR 2027ff	AMLR Art. 13(1)(a)
PID	Nationality / Citizenship	natural person can be UBOs or Initiator (legal repr, signatory rights, mandate person)	EU-AMLR 2027ff	AMLR Art. 13(1)(a)
PID	Place of birth	natural person can be UBOs or Initiator (legal repr, signatory rights, mandate person)	EU-AMLR 2027ff	AMLR Art. 13(1)(a)
PID	Residential address (natural persons)	natural person can be UBOs or Initiator (legal repr, signatory rights, mandate person)	Other (please comment)	Civil registry

Attestation Scheme	Data Point	Description	Required by	Regulation
SAE	SAE sector (Italy only)	type of economic structure	Other (please comment)	AMLR Art. 15; RTS §34
SignatoryRights (non-BU1)	Applicable EUID	Legal entity for which the signatory rights are valid	Other (please comment)	Bank Internal Req.
SignatoryRights (non-BU1)	Email	The email of the employee	Other (please comment)	Bank Internal Req.
SignatoryRights (non-BU1)	Full name	Full name of the employee	Other (please comment)	Bank Internal Req.
SignatoryRights (non-BU1)	Person ID	Government Issued ID	Other (please comment)	Bank Internal Req.
SignatoryRights (non-BU1)	Phone	The phone number of the employee	Other (please comment)	Bank Internal Req.
SignatoryRights (non-BU1)	Role	The role of the employee	Other (please comment)	Bank Internal Req.
SignatoryRights (non-BU1)	Site Information	Additional site information of the legal entity	Other (please comment)	Bank Internal Req.
SoW	Source of Wealth (SoW)	see Data Point	EU-AMLR 2027ff	Art. 34 AMLR
Tax ID	Tax number	identification number assigned by a country's tax authority (Tax/TIN)	EU-AMLR 2027ff	Art. 22(1)(b), Recital 23 AMLR
Tax ID	Tax Residency	tax_residency_country	EU-AMLR 2027ff	Art. 22(1)(b) AMLR
TFS	TFS (targeted financial sanctions) Screening Persons to be Covered	Screening of sanction lists happens after receiving attestations. For the MVP we will not include risk analysis and sanction list screening in the scope. Therefore not needed for scenario 1 & 4.	EU-AMLR 2027ff	Art. 30 RTS
TrustInstrumentInfo	Type of trust / foundation	<to be explained in more detail>		
UBO List	All Nationalities	see Data Point	EU-AMLR 2027ff	AMLR Art. 62
UBO List	All types and scope of economic interests	see Data Point	EU-AMLR 2027ff	AMLR Art. 62
UBO List	Birthdate	see Data Point	EU-AMLR 2027ff	AMLR Art. 62

Attestation Scheme	Data Point	Description	Required by	Regulation
UBO List	Control %	Control % of natural person e.g sourced from Transparenzregister	EU-AMLR 2027ff	AMLR Art. 62
UBO List	Country of residence	see Data Point	EU-AMLR 2027ff	AMLR Art. 62
UBO List	Document-number	<to be explained in more detail>	EU-AMLR 2027ff	AMLR Art. 62
UBO List	Full Name	see Data Point	EU-AMLR 2027ff	AMLR Art. 62
UBO List	Homeadress	see Data Point	EU-AMLR 2027ff	AMLR Art. 62
UBO List	Location of Birth	see Data Point	EU-AMLR 2027ff	AMLR Art. 62
UBO List	Names of UBOs (≥25%) or relevant control	Defined as UBOs in the Registers (≥25%) and/or the UBOs (≥25% - in the calculation rule 1,2,3)	EU-AMLR 2027ff	Art. 61–63 AMLR
UBO List	Ownership %	shares held by natural person	EU-AMLR 2027ff	AMLR Art. 62
UBO List	personal identification number	see Data Point, compare PID	EU-AMLR 2027ff	AMLR Art. 62
VAT ID	VAT registra- tion number	Number issued to businesses that are registered to collect VAT	EU-AMLR 2027ff	Art. 22(1)(b), Recital 23 AMLR

Appendix 2: PA3 MVP Partner Overview

PA3 MVP		Holder (EUBW)									
Attestation type	Issuer	Bosch (DE)	Bosch (NL)	SBB (CH)	Sole Trader (NL)	Voestalpine (AT)	Bank ID (CZ)	Deutsche Bahn Cargo (DE)	Leone SRL (IT)	Sole Trader (PL)	Deutsche Bank (DE)
EBWOID (LPID)	Business Register	Bundesanzeiger	KVK	Bundesanzeiger	KVK	Bundesanzeiger	Bundesanzeiger	Bundesanzeiger	Infocert	Ministry of Development	Bundesanzeiger
EUCC	Business Register / BRIS	Bundesanzeiger	KVK	Bundesanzeiger	KVK	Bundesanzeiger	Bundesanzeiger	Bundesanzeiger	Infocert	Ministry of Development	Bundesanzeiger
EU PoA (MVP+)	Self-attestation or PubEAA or QEAA	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	Self-issued	Not required
PID	Member State	EUDI Wallet ¹ ; Governikus	EUDI Wallet ² ; DigIDentity	EUDI Wallet ³	EUDI Wallet ⁴	EUDI Wallet ⁵	EUDI Wallet (Aricoma)	EUDI Wallet ⁶	Italian EUDI Wallet in WE BUILD?	Tbd: Any PID / EUDI Wallet provider ⁷	Not required

¹With synthetic Attestation

²With synthetic Attestation

³Holding Swiss SWIYU ID

⁴With synthetic Attestation

⁵To be confirmed with Governikus; will be a german citizen opening bank account

⁶To be confirmed with Governikus

⁷Fallback option: EUDI reference

PA3 MVP		Holder (EUBW)									
Attestation type	Issuer	Bosch (DE)	Bosch (NL)	SBB (CH)	Sole Trader (NL)	Voestalpine (AT)	Bank ID (CZ)	Deutsche Bahn Cargo (DE)	Leone SRL (IT)	Sole Trader (PL)	Deutsche Bank (DE)
TAX NR (Company) ¹		Optional ²		Optional ³	KVK	Optional ⁴	Optional ⁵	Optional ⁶	Optional ⁷	Ministry of Development	Not required
TAX ID	Central / National Tax Office	Not relevant	Not relevant	Not relevant	?			Not relevant			Not required
VAT	Self-issued ⁸	National register ⁹ , else self-issued or Bundesanzeiger	Tax administration (NL)	Bundesanzeiger	?	Bundesanzeiger	Bundesanzeiger	Bundesanzeiger	Infocert	?	Not required
Contact Person	EAA-Attestation	Self-issued	Self-issued	Self-issued	Not required	Self-issued	Self-issued	Self-issued	Self-issued	Not required	Not required

¹Tax Number or VAT or LEI (minimum one needed)

²Could be company declared (manual input)

³Could be company declared (manual input)

⁴Could be company declared (manual input)

⁵Could be company declared (manual input)

⁶Could be company declared (manual input)

⁷Could be company declared (manual input)

⁸Optionally National Register or Tax administration

⁹Ministry of Finance; discussion with Bundesanzeiger and MoF ongoing

PA3 MVP		Holder (EUBW)									
Attestation type	Issuer	Bosch (DE)	Bosch (NL)	SBB (CH)	Sole Trader (NL)	Voestalpine (AT)	Bank ID (CZ)	Deutsche Bahn Cargo (DE)	Leone SRL (IT)	Sole Trader (PL)	Deutsche Bank (DE)
Company Info	EAA-Attestation	Self-issued	Self-issued	Self-issued	Not required	Self-issued	Self-issued	Self-issued	Self-issued	Not required	Not required
LEI (MVP+)		Bundesanzeiger / KVK	Bundesanzeiger / KVK	Bundesanzeiger / KVK		Bundesanzeiger / KVK	Bundesanzeiger / KVK	Bundesanzeiger / KVK	Infocert		Not required
UBO List	EAA-Attestation	Self-issued	Self-issued	Self-issued	Not required	Self-issued	Self-issued	Self-issued	Self-issued	Not required	Not required
UBO List TP ¹		Bundesanzeiger	KVK	Not provided ²	Not required	Bundesanzeiger	Bundesanzeiger	Bundesanzeiger	Infocert	Not required	Not required
Owner List	EAA-Attestation ³	Self-issued	Self-issued	Self-issued or Bundesanzeiger	Not required	Self-issued or Bundesanzeiger	Self-issued or Bundesanzeiger	Self-issued or Bundesanzeiger	Self-issued	Not required	Not required
Control List	EAA-Attestation	Self-issued	Self-issued	Self-issued or Bundesanzeiger	Not required	Self-issued or Bundesanzeiger	Self-issued or Bundesanzeiger	Self-issued or Bundesanzeiger	Self-issued	Not required	Not required
Signatory Rights	EAA-Attestation	Self-issued	Self-issued	Self-issued	Not required	Self-issued or Bundesanzeiger	Self-issued or Bundesanzeiger	Self-issued	Self-issued	Not required	Not required

¹Transparency Register

²CH does not have a Transparency Register – banks need to keep manual process as no registry exists

³QEAA

PA3 MVP		Holder (EUBW)									
Attestation type	Issuer	Bosch (DE)	Bosch (NL)	SBB (CH)	Sole Trader (NL)	Voestalpine (AT)	Bank ID (CZ)	Deutsche Bahn Cargo (DE)	Leone SRL (IT)	Sole Trader (PL)	Deutsche Bank (DE)
Signature Process ¹		QTSP (D-Trust/QES)	QTSP (DigIDentity/QES)	QTSP	?	QTSP	QTSP	QTSP		?	QTSP (Germany)

¹EUDI Wallet

WE BUILD consortium

Specification Scenario 2 – Digital Signatures

WP3 – PA3

Date : 19-06-2026
Version : (<0.7 = draft; 0.7 = for review; 0.8 = reviewed; 1.0 = final)
Status : 1.0 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>
1.3	<i>Known open points.....</i>	<i>3</i>
2	Scenario specification	4
2.1	<i>Introduction.....</i>	<i>4</i>
2.2	<i>Scenario pre-conditions</i>	<i>4</i>
2.2.1	<i>MVP Restrictions</i>	<i>5</i>
2.3	<i>Scenario main flow.....</i>	<i>6</i>
	<i>Company Perspective</i>	<i>6</i>
2.4	<i>Scenario additional flows</i>	<i>7</i>
2.5	<i>Challenges and barriers.....</i>	<i>8</i>
2.6	<i>Working Assumptions.....</i>	<i>8</i>
3	Detailed scenario flow	9
4	Roles and participants.....	11
4.1	<i>Scenario roles and participants</i>	<i>11</i>
4.2	<i>Additional roles and partners.....</i>	<i>11</i>
4.3	<i>Target country combinations</i>	<i>12</i>
4.4	<i>Requirements</i>	<i>12</i>
5	Attestations	13
5.1	<i>Introduction.....</i>	<i>13</i>
5.2	<i>Attestations to be provided by other UCs/WGs/scenarios</i>	<i>13</i>
5.3	<i>Created attestations in the scenario</i>	<i>13</i>
	Annex 1 – Requirements for scenario roles	14

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 2, as part of use case PA3, Corporate Banking, 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

This MVP scenario focuses on enabling remote contract signing using credentials issued and validated within the EUDI Wallet and EU Business Wallet ecosystem.

The scenario is based on the following documentation:

- The WE BUILD Architecture & Integration Blueprint [WE BUILD — Architecture & Integration Blueprint \(D4.1\)](#), in particular paragraph 4.3;
- Cloud Signature Consortium specification for remote signing with wallets CSS API v2.2: [CSC API V2.2 | Cloud Signature Consortium](#)
- German EUDI Wallet Function: Qualified Electronic Signature (QES) [QES - Blueprint for the EUDI Wallet Ecosystem in Germany](#)
- PA3 Stock Taking document: <https://portal.webuildconsortium.eu/group/14/files/5922/collaboration/view/3932>
- PA3 Attestation requirements: <https://portal.webuildconsortium.eu/group/14/files/6698/collaboration/edit/4072>
- Business Wallet Regulation: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0838>
- ARF: <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework>

1.3 [Known open points](#)

Date	Topic (Page)	Proposed	Solution
N/A			

2 Scenario specification

2.1 Introduction

This scenario, which commences after a customer has completed the onboarding process of a bank, seeks to extend the banking onboarding flow tested in Scenario 1 from PA3, WP2. Once the customer onboarding process has been successfully completed, the holder will be asked to sign the legal agreement between the legal person and the bank to open the bank account.

Scenario 2 seeks to deliver the integration of wallet-based signatures and authentication for both the legal person (EU Business Wallet) and the natural person (EUDI Wallet (PID)) acting on behalf of the legal person.

For the purpose of signing the contract with the Bank, it is not necessary to issue a Signatory Rights attestation as initially assumed. Further research has shown that the contract for the bank account can be signed by the Legal Representatives of the customer. The names of these signatories are included in the EUCC.

2.2 Scenario pre-conditions

The first pre-condition for being able to start testing scenario 2 is the completion of scenario 1. For example, scenario 2 does not require involvement from Business Registries as authentic sources for legal person attestations, like the EUCC, as these will be issued and collected as part of scenario 1. There are no attestations issued as part of scenario 2. There is a requirement for QTSPs to issue a Qualified Electronic Signature (QES) to the EUDI Wallets of the legal representatives that are mandated to sign the bank account agreement on behalf of the company.

As the Legal Representatives will be signing on behalf of the company, both their PID and the EBWOID are to be included in the transaction data presented to the user. This joint presentation still needs to be defined.¹

By replacing the Signatory Rights attestation by the EUCC, the pre-conditions for Scenario 2, are now somewhat different from the PA3 Stock Taking document, section 1.6:

1. Updated: For signing the contract with the bank, there is no longer a need for a 'Signatory Rights' attestation; the EUCC is sufficient for identifying legal representatives and their identities can be verified using the PIDs for their EUDI Wallets..
2. Trust Framework: An accessible and defined trust framework in coordination with WP4.
 - Interoperability Environment: Connection to the WP4 test environment including test cases and test data (e.g represented company & credentials)

¹ WE BUILD Architecture & Integration Blueprint, paragraph 4.3.4

- Technology Provider: Issuer, holder, and verifier capabilities must follow the **WE BUILD Architecture Blueprint** and **eIDAS 2.0** standards. At least two wallet providers from different countries to validate dual-wallet interoperability.
- At least two QTSPs from different countries are needed to issue QES to the EUDI Wallets of the Legal Representatives of the company so they can sign the contract to open the bank account.
- Joint agreement on required **data schemas structure** (via the semantics group) to ensure cross-use-case alignment.
- Identification and resolution of functional gaps discovered during prototyping.
- Sandbox setup: Controlled pre-production environment accessible to testers outside the bank, with monitoring and audit capabilities. To be discussed if this shall be provided via Testing.
- Accessibility and security: Compliance with the European Accessibility Act and banking security policies during pilot operations.
- Document signing is possible within the business wallet, but only if the business wallet is set up as a Signature Creation Application to create a hash of the document that needs signing.

2.2.1 MVP Restrictions

1. **Reduced Verification & Trust Reliance:** Neither seller 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:** 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, 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

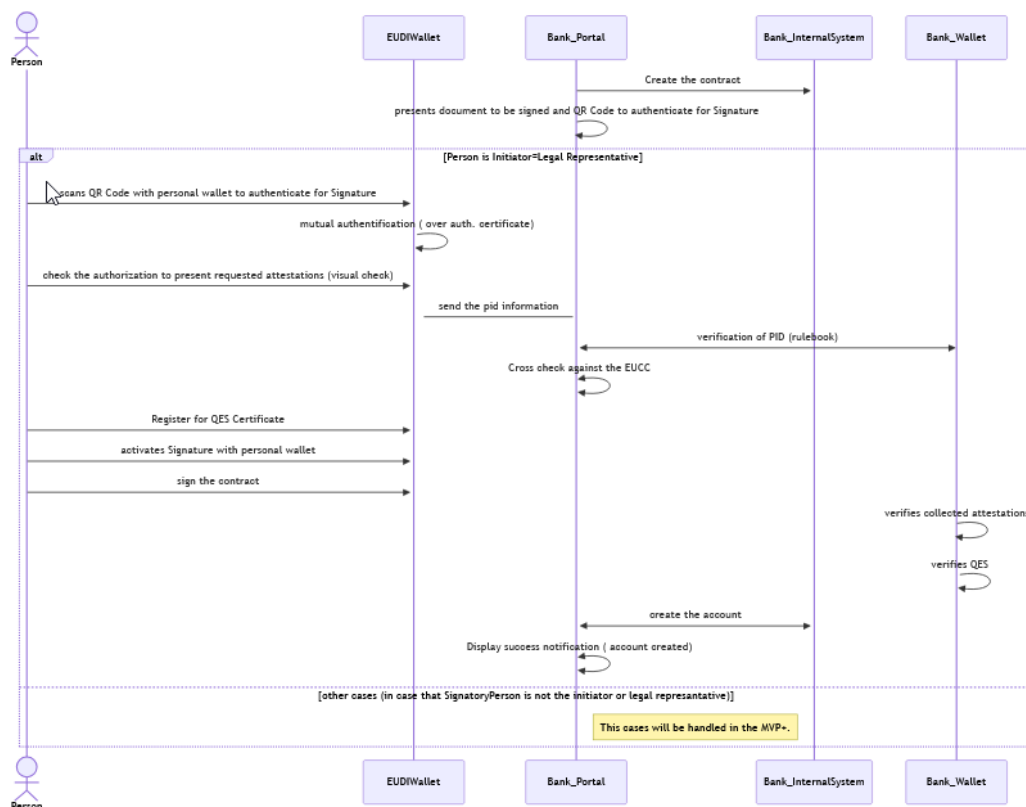
use cases involving sensitive data within the MVP and requires careful management of data exposure.

2.3 Scenario main flow

For the MVP the following restriction are available

Company Perspective

- The person who initiated the account opening process is also: legal representative, UBO and contact person (to make it simple: 4 positions in 1; one-person GmbH in Germany, covering SME-cases)
- The initiator is the sole legal representative, who is also the person which will sign the contract for the bank relationship (one-person GmbH in Germany, covering SME-cases).



Scenario 2: Contract Signing – process steps:

- The bank selects one or multiple Legal Representatives from the EUCC attestation shared by the customer for signing the contract.
- The bank prepares the contract, and includes the names of the relevant Legal Representatives that need to sign
- The bank shares a sign request for the contract with the legal representatives from the Bank Portal.

- The Legal Representatives share their PID attestation from their EUDI Wallet.
- The bank BW verifies the Legal Representatives based on their PID .)
- The legal representatives sign the contract within the Bank Portal using the QES from their EUDI Wallet
- Once completed, the signed contract is shared back to the BW of the company by the BW of the Bank. Note that the bank does not need to counter sign the contract.
- The bank account is created and notification is shared with the company from the Bank Portal.

For the MVP+ there is no restriction in regard to the initiator.

2.4 Scenario additional flows

A second flow would be for the bank account contract to be shared between the BW of the bank and the BW of the company. This scenario could be set up as follows:

- The bank selects one or multiple Legal Representatives from the EUCC attestation shared by the customer for signing the contract.
- The bank prepares the contract, and includes the names of the relevant Legal Representatives that need to sign.
- The bank shares the contract from it's own BW to the BW of the company
- The company creates a sign flow within the BW and invites the Legal Representatives to sign with their QES in their EUDI Wallets
- Once completed, the signed contract is shared back to the BW of the Bank by the BW of the company. Note that the bank does not need to counter sign the contract.
- The bank account is created and notification is sent to the company.

Flow	Short description
Variations	
Remote Signing with Local SCA (BW Wallet as SCA)	The bank employee initiates signing of the bank account contract from the banks' BW, which also acts as the Signature Creation Application (SCA).
Local signing (EUDI Wallet as SCA)	The user (legal representative) initiates signing from their EUDI wallet, which also acts as the SCA. The document is presented to the user within their wallet for review and consent.
Exceptions	
-	

2.5 Challenges and barriers

The first prerequisite that enables the testing of scenario 2 is the successful completion of scenario 1, account opening. The main risks, as outlined in paragraph 1.7 of the PA3 Stock Taking document, are inhibitors for scenario 1. Once scenario 1 is completed, we need to cover the following roles for at least 2 countries from scenario 2's perspective:

- Companies as business wallet holders
- Business wallet providers
- Natural person wallet providers (to be used by Legal Representatives)
- Qualified Trust Service Providers (for QES issuance)
- Banks as Relying Parties/Verifiers.

2.6 Working Assumptions

As a starting point for the specification of this scenario, a working assumption has been made to select a **Wallet-Centric model**: the Wallet creates a signed document or just the signature, supported by a QTSP for the cryptographic signature value.

The other option, using a **QTSP-centric model** whereby the user uses the Wallet to authorizes a QTSP to sign a document on their behalf can also be made available for testing..

Within the Wallet-Centric model; the use case and scenario leads have selected the 'Remote Signing with External Signature Creation Application (SCA)' option. This means that the user initiates signing from the wallet, while the SCA (i.e. Bank Portal) is external. The document (contract) is 'sent to' (or shared the external SCA for review and consent, after which the signing request is forwarded to a remote SCD that creates the signature and returns the result.

The 'WE BUILD Architecture & Integration Blueprint' describes 2 other wallet-centric options that are will be considered as possible fall-back wallet-centric scenarios for the MVP scenario 2:

2. Remote Signing with Local SCA (Wallet as SCA), whereby the user initiates signing from the wallet, which also acts as the SCA. The document is presented to the user within the wallet for review and consent. After approval, the wallet forwards the signing request to a remote SCD that produces the signature and returns the result
3. Local signing, whereby the user initiates signing from the wallet, which also acts as the SCA. The document is presented to the user within the wallet for review and consent. After approval, the signature is created locally using a SCD integrated in the user's device.² This is the least preferred option for now.

² WE BUILD Architecture & Integration Blueprint, paragraph 4.3.1 and 4.3.2

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
Holder shares EUCC from BW with Relying Party BW (part of scenario 1)	Holder BW; Relying Party	Holder BW employee shares EUCC Attestation from BW to Verifier BW	Secure communication and sharing of a document between BWs is t.b.d.	
Verifier retrieves signatory information from Holder EUCC	Relying Party; Holder BW	The bank employee (verifier) is triggered by the banking system to confirm Legal Representatives listed on the EUCC	The bank employee can access the EUCC and derive the Legal Representatives	
Verifier creates bank account contract	Relying Party	The contract for the bank account is created by the bank and the names of the Legal Representatives are included for signing.	The banking portal or a customer specific dashboard can be made available for contract signing.	QTSP-centric Signing Model
Verifier presents document to be signed	Relying Party	The contract is presented in the bank portal to be signed incl. QR code to authenticate for Signature	Bank portal is set up to act as Signature Creation Application (integrate with CSC2.2)	QTSP-centric Signing Model
Natural Person (Legal rep) authenticates with EUDI Wallet	Holder EUDI Wallet, Relying party	Legal representative accesses the bank portal, authenticates via EUDI Wallet by sharing PID	WUA EUDI Wallet and RP Certificates for bank portal enable mutual authentication	
Relying party verifies Legal Rep	Relying party	Bank verifies identity of LR from PID and matches to EUCC		Signatory Rights attestation

Legal Rep requests QES and activates via EUDI Wallet	Holder EUDI Wallet	PID & Hash of bank contract + PIN are sent to rQSCD	Bank portal as SCA can hash document	QTSP-centric Signing Model
Legal Rep signs contract from EUDI Wallet	Holder EUDI Wallet	RQSCD signs hash and returns document to SCA.	Bank portal as SCA can 'unpack' signed hash and include QES from Legal Rep on document	QTSP-centric Signing Model
Success Notification	Relying party	Legal Rep is shown success notification in bank portal	Bank portal as SCA confirms signing transaction completed	QTSP-centric Signing Model
Signed contract shared	Relying party Holder BW	Signed and completed contract copy (pdf) is sent to the BW of Holder.		Document could be shared via QERDS from Bank BW to Holder BW

4 Roles and participants

4.1 Scenario roles and participants

The roles that are relevant for this scenario, and list which of the partners will play this role in piloting the scenario are included in the table below.

Primary role	UC partner Name	Country
1. User of EUDI Wallet	For Legal Representatives from Holder (Bosch NL, Bosch DE, Identonic POL). Signs the bank account contract within the Bank Portal of the RP with QES from their EUDI Wallet	DE, NL, POL
2. Authentic sources	N/A, (EUCC will be issued as part of PA3 Scenario 1 (by Bundesanzeiger Verlag, KvK, and Polish Business Registry (for sole traders – CEIDG)	DE, NL, POL
3. Relying party	Deutsche Bank ABN AMRO (TBC) Polish Bank (Pekao SA - TBC) Service = bank account contract creation and signature flow initiation	DE, NL, POL
4. Intermediary	N/A (for now)	
5. User of EU BW	Bank employee (Deutsche Bank, ABN AMRO (TBD), Pekao SA (TBD)) and holder employee (Bosch NL, Bosch DE, Identonic POL).	DE, NL, POL

4.2 Additional roles and partners

The partners from WE BUILD Work Package 4 that have confirmed their participation in this scenario are included in the table below. This number may change once testing commences.

Primary role	UC partner Name	Country	Wallet
1. EUDI Wallet provider	Digidentity B.V. Procivis Other TBD (DE, POL)	NL, AT, EU	NW
2. EU BW provider	Credenco (NL) Spherity (DE) Procivis Other (POL TBD)	NL, DE	BW
3. PID Provider	Digidentity (Q-PID for now) Bundesdruckerei (DE)	NL, EU	NW

	PESEL / Ministry of Digital Affairs (POL) - tbc		
4. Trusted list registrar	WE BUILD Trust Registry Infrastructure	N/A	N/A
5. QEAA provider	Digidentity B.V. PWPW D-TRUST(tbc)	NL, POL, DE	NW/BW
6. Pub-EAA provider	KvK, Bundesanzeiger Verlag, CEIDG	NL, DE, POL	NW/BW
7. EAA provider	N/A		
8. QES provider	Digidentity B.V. PWPW D-Trust	NL, Pol, DE	NW

4.3 Target country combinations

The countries that will participate in cross-border piloting of scenario 2 are listed in the table below.

Relying Party country	Issuing Country		
	DE	NL	POL
DE			
NL			
POL			

4.4 Requirements

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

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

The Declare which attestations that will be used in the scenario, but will NOT be designed, implemented and issued to wallet within the scenario are listed in the table below.

Attestation name	Short description	To be provided by	For Countries	Requirements
EUCC	Names of legal representatives from BW of bank customer for setting up contract sign flow.	Business Registries	DE, NL, POL	Single or joint signing authority needs to be clear for Legal Representatives.
PID	Personal Identification data for Legal Representatives of holder company	PID group or PID issuers	DE, NL, POL	

5.3 Created attestations in the scenario

N/A

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
1. User of EUDI Wallet	a. Legal representatives of customer need request and create QES from their EUDI Wallet for signing bank account contract
	b. PID from EUDI Wallet will be used to
	c.
2. Authentic sources	a. Issues EUCC (as part of Scenario 1) that will be used to derive the names of the Legal Representatives
	b.
	c.
3. Relying party	a. Bank needs to have a Business Wallet (BW)
	b. Issue contract for signing from BW
	c. Bank portal to act a a Signature Creation Application
4. Intermediary	a. N/A
	b.
	c.
5. EUDI Wallet provider	a. Legal representatives need an EUDI Wallet with PID and QES for signing bank account contract (QTP flow) or ability to request QES from EUDI Wallet.
	b.
	c.
6. PID Provider	a. Issues PID to EUDI Wallet of Legal Representatives
	b.
	c.
7. Trusted list registrar	a. TBC – for now use WE BUILD Trust Registry Infrastructure
	b.
	c.
8. QEAA provider	a. Same as Authentic Source – needs to issue the EUCC (on behalf of business register) as a QEAA (if needed)
	b.
	c.
9. Pub-EAA provider	a. Same as Authentic Source – needs to issue the EUCC as a PUB-EAA
	b.
	c.
10. EAA provider	a. N/A
	b.
	c.
11. QES provider	a. Issue QES to Legal Representatives upon presentation of PID.
	b.

WE BUILD consortium

Specification Scenario 3 – IBAN Ownership Verification

WP3 – PA3 (Corporate Banking)

Date : 19.06.2026
Version : 1.0
Status : final

Table of Contents

1 Introduction.....	3
1.1 Objectives of this document	3
1.2 Scenario introduction.....	3
1.3 Known open points.....	4
2 Scenario specification – Scenario 3	4
2.1 Introduction	4
2.2 Scenario pre-conditions	5
2.2.1 MVP Restrictions	5
2.3 Scenario main flow.....	6
2.4 Scenario additional flow (MVP+).....	7
2.5 Challenges and barriers	8
2.6 Working Assumptions	8
3 Detailed scenario flow	9
4 Roles and participants	10
4.1 Scenario roles and participants.....	10
4.2 Additional roles and partners	10
4.3 Target country combinations.....	10
4.4 Requirements.....	11
5 Attestations	11
5.1 Introduction	11
5.2 Attestations to be provided by other UCs/WGs/scenarios.....	11
5.3 Created attestations in the scenario	12

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 3, as part of use case PA3 in work package 3 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

Scenario 3 (PA3) describes the process for triggering and issuing an IBAN Ownership Verification (IBAN-OV) attestation via the European Business Wallet. The IBAN-OV attestation provides trusted assurance to third parties that a specific IBAN is legally owned by a designated **legal entity**.

The scenario is based on the following documentation:

- **WP4 Architecture Blueprint:**
<https://webuild-consortium.github.io/wp4-architecture/blueprint/blueprint.html>
- **BU1 Stock taking document:**
<https://portal.webuildconsortium.eu/group/3/files/5921/collaboration/view/2449>
- **PA3 Stock taking document:**
<https://portal.webuildconsortium.eu/group/14/files/5922/collaboration/view/3932>
- **PA3 Attestation requirements:**
<https://portal.webuildconsortium.eu/group/14/files/6698/collaboration/edit/4072>
- **PA3 IBAN-OV Attestation:**
<https://portal.webuildconsortium.eu/group/14/files/6861/collaboration/edit/3335>

2 Scenario specification – Scenario 3

2.1 Introduction

Scenario 3 (PA3) of the WE BUILD consortium covers the process for triggering and issuing an IBAN Ownership Verification (IBAN-OV) attestation. The IBAN-OV attestation provides trusted assurance to third parties that a specific IBAN is legally owned by a designated legal entity (or sole traders which are registered in a national register). This verified proof of ownership can be used across various business processes (e.g. onboarding process) to reduce errors and mitigate fraud risks. This attestation will not be used to initiate or execute any kind of payment.

The IBAN-OV attestation will be provided within the Relying Party registration process (linkage to BU1 – Scenario 1 & 6) for the MVP, or upon request from the legal entity owning the IBAN account, at a later date after the account opening process for the MVP+.

Once issued and securely stored in the EBW wallet, the IBAN-OV attestation can be reused for multiple transactions as long as it will not be revoked. This increases operational efficiency while ensuring continued compliance with banking regulations and applicable legal standards.

This scenario covers the issuance of an IBAN-OV attestation as an EAA directly by the bank, which acts as both Credential Issuer and Authentic/Primary Source and is sufficient for the majority of domestic and cross-border business contexts. This will be tested within the MVP and the Rulebook can be found [here](#).

2.2 Scenario pre-conditions

The scenario considers the following pre-conditions:

The EUDI Wallet and the EBW are installed, operational and hold an issued PID, EBWOID, EU Company Certificate (EUCC), Signatory Rights, Power of Attorney or Power of X attestations in the respective wallet. All held attestations are active and valid.

For this scenario, we built upon a successful account opening from PA3, Scenario 1 and 2 (including BU1, Scenario 1) and all of its required attestations (e.g. contact persons/person initiating the relationship) The issuance of the IBAN-OV attestation is done directly after the account opening, while still being logged into the bank's portal (thereby skipping Phase 0).

2.2.1 MVP Restrictions

- **Reduced Verification & Trust Reliance:** Neither seller 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 (trust infrastructure) 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 member states have explained that only QTSPs can be included in the TLOL (Trusted list of lists) also due to scalability reasons. Accordingly, the WE BUILD-specific TLOL is not applicable outside of the consortia, 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.

2.3 Scenario main flow (MVP)

The main flow focuses on the issuance of an IBAN-OV attestation as an EAA, self-issued by the bank in its dual role as Credential Issuer and Authentic/Primary Source. The attestation is requested by the sole legal representative of Company A for an already established and active account.

For this scenario the following restriction/prerequisites are available:

- The process is executed directly after the successful account opening process by the initiating person (session still active)
- This person is the sole legal representative for the bank relationship (one-person GmbH in Germany, covering SME-cases).
- The process ending with the triggering and issuance of the IBAN-OV attestation as EAA.

An overview of this Scenario is presented here:

1. The employee initiates IBAN-OV issuance service via the bank's portal (an account already exists for the Company A)
2. Identification process of the employee using their EUDI Wallet in combination with the Company A's EBW, confirming both their identity and their authorisation to act on behalf of Company A (Phase 0) is skipped (due to the active session from the account opening)
3. The bank solicits an attestation offering and the IBAN-OV attestation is issued to the EBW of the Company A.

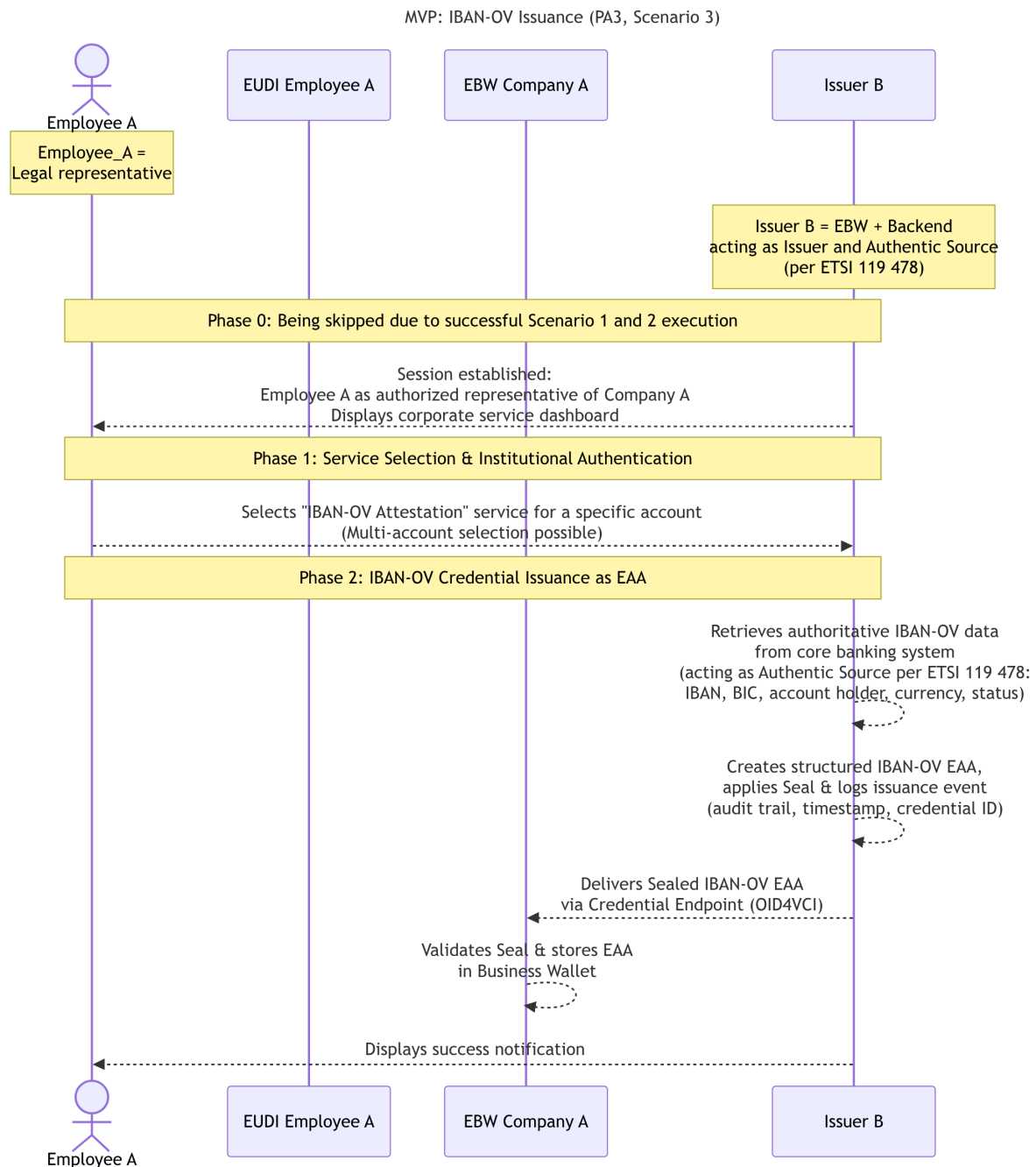


Figure 1: [IBAN-OV Issuance](#)

2.4 Scenario additional flow (MVP+)

For the MVP+, we pilot the asynchronous IBAN-OV attestation issuance. In contrast to the MVP, this process is not triggered directly after account opening.

For the MVP+ the following restriction are available:

- The process is triggered “weeks” after the successful account opening process resulting in re-occurring mutual authentication.
- Any authorised person (having the required attestations e.g. Signatory Rights, PoA/PoX in the respective EBW and linked to this specific person) is able to

trigger the process (in contrast to the MVP where the sole legal representative triggers the issuance).

- the process ending with the triggering and issuance of the IBAN-OV issuance/attestation as EAA.

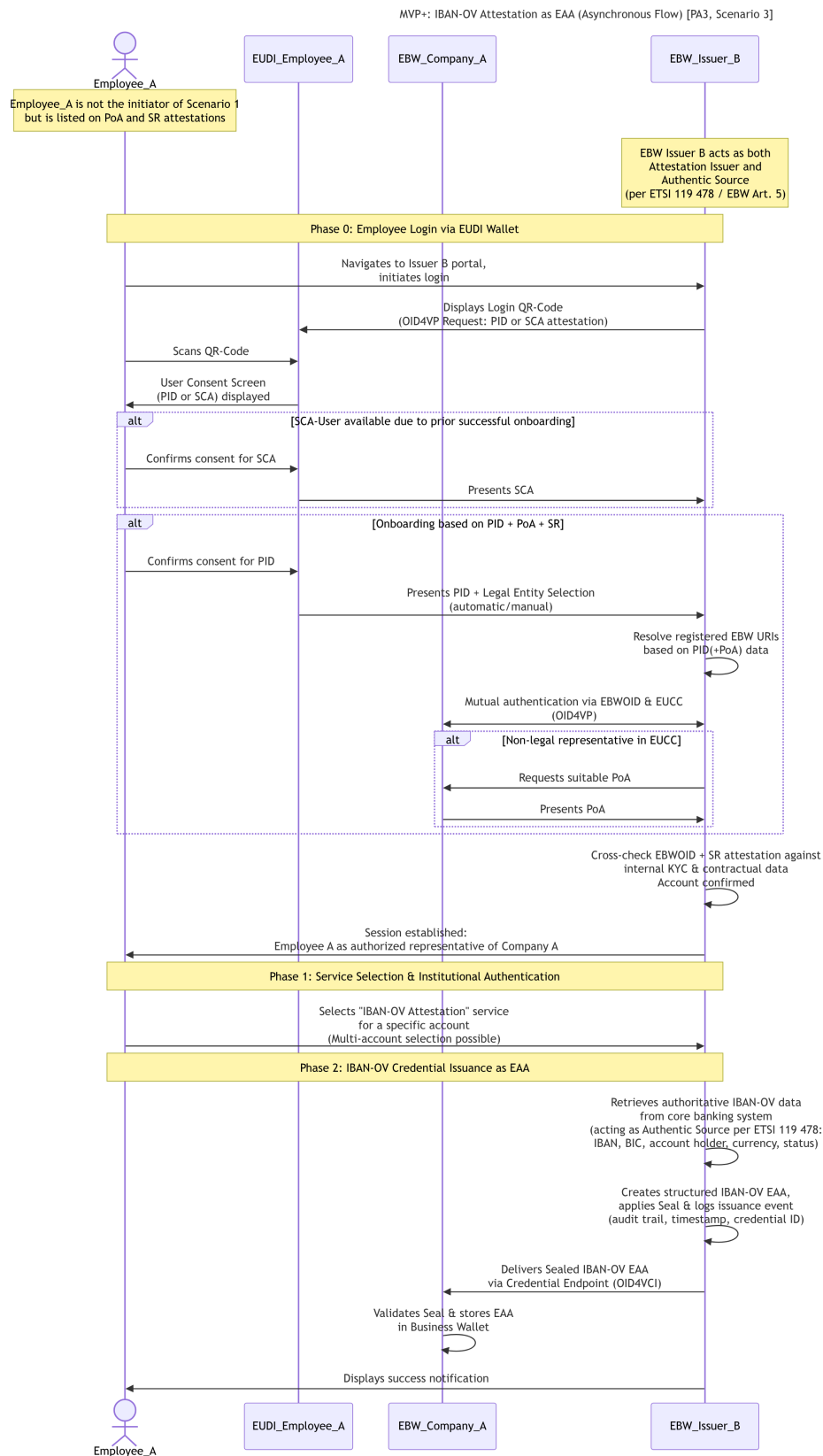


Figure 2: IBAN-OV Issuance (asynchronous; github link to be added when figure lands in official repo)

2.5 Challenges and barriers

Challenges in regard to the timeline arise as we are dependent on the results from BU1 + PA3, Scenario 1. Without a finalized BU1, Scenario 1, the subsequent flows and scenarios in PA3 are at risk.

From our current point of view, there are minimal to no barriers. Our work is built on the results from EWC, and we have already received preliminary approval from the Semantic group. Initial feedback from a smaller group within PA3 & PA4 has already been incorporated.

2.6 Working Assumptions

We are piloting the interplay of EUDI and EBW wallets, resulting in any on boarding business having an EBW wallet for the legal entity and an EUDI Wallet for the natural persons acting on behalf of the company.

Furthermore, the scenario considers the following pre-conditions as illustrated in Section 2.2.

The EUDI Wallet and the EBW are installed, operational, and hold an issued PID, EBWOID, EU Company Certificate (EUCC), Signatory Rights, Power of Attorney, or Power of X attestations in their respective wallets. All held attestations are active and valid.

We are building upon a successful account opening from PA3, Scenario 1+2 (including BU1, Scenario 1) and all of its required attestations (e.g., contact persons/person initiating the relationship) prior to our scenario.

3 Detailed scenario flow

Per step in the main flow (MVP), 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
Phase 0: Login & Authorization	Employee_A	This Phase 0 is being skipped due to a successful Scenario 1 and 2 execution		
Phase 1: Service Selection & Institutional Authentication	Employee_A	Selects “IBAN- OV Attestation” service for a specific account (multi-account selection possible)		
Phase 2: IBAN- OV Credential Issuance as EAA	Issuer_B	Retrieves authoritative IBAN-OV data from core banking system		(acting as Authentic Source per ETSI 119 478: IBAN, BIC, account holder, currency, status)
		Creates structured IBAN-OV EAA, applies AdSeal (self-issued EAA) & logs issuance event (with audit trail, timestamp, credential ID)		
		Delivers AdSealead IBAN-OV EAA via Credential Endpoint (OID4VCI)		
	EBW_Company_A	Validates AdESeal & stores EAA in Enterprise Wallet		

Main flow step - same-device website to app	Actor	Interpretatio n or reference	Dependencies	Variations and exceptions
	Issuer_B	Displays success notification to Employee-A		

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
1. User of Wallet (=Holder)	Robert Bosch B.V.	NL
2. Issuer	Deutsche Bank AG	DE

4.2 Additional roles and partners

Primary role	UC partner Name	Countries	Wallet
1. EUDI Wallet provider	Procivis GmbH	DE	NW
2. EBW Provider	Spherity GmbH	DE	BW

4.3 Target country combinations

		Issuing country		
		DE	NL	...
Relying party country	DE			
	NL	X		
	...			

4.4 Requirements

The section 2.5 (Challenges and barriers) 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	Annex 1	Authentic Source	DE, NL	
EUCC	Annex 1	Authentic Source	DE, NL	
TAX Number	Annex 1	Authentic Source	DE	
TAX ID	Annex 1	Authentic Source	DE	
UBO List	Annex 1	EAA - Attestation	DE	
Control List	Annex 1	EAA - Attestation	DE	
Ownership List	Annex 1	EAA - Attestation	DE	
LEI	Annex 1	Authentic Source	DE	
Company Info	Annex 1	EAA - Attestation	DE	
Contact Person	Annex 1	EAA - Attestation	DE	
Signatory Rights	Annex 1	EAA - Attestation	DE	

5.3 Created attestations in the scenario

EAA – Attestation issued by the bank out of their Business Wallet

Attestation name	Short description	For Countries	Applicable domain standards
IBAN-OV Attestation	Refer to chapter 2.1	all	EAA

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.
	b.
	c.
2. Authentic sources	a.
	b.
	c.
3. Relying party	a.
	b.
	c.
4. Intermediary	a.
	b.
	c.
5. EUDI Wallet provider	a.
	b.
	c.
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.

WE BUILD consortium

Specification PA4 Scenario 1.1 _ card payment _ deferred invoice

WP3 – PA4 (Corporate Payments)

Date : 20.June.2026
Version : 1.0
Status : FINAL

Index

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
2.3	Scenario main flow	7
2.4	Challenges and barriers	9
2.5	Working Assumptions	9
2.5.1	Seller (Holder)	9
2.5.2	Buyer (Relying Party).....	9
2.5.3	Authorised Person.....	9
2.5.4	Holder Business Wallet	10
2.5.5	Relying-Party Business Wallet.....	10
2.5.6	General.....	10
3	Detailed scenario flow.....	10
3.1	Step 1: Legal Entity Selection	10
3.2	Step 2: Payment Initiation.....	11
3.3	Step 3: Payment Authorization	11
3.4	Step 4: Legal Entity Payment Authorization.....	11
3.5	Step 5: Payment Settlement.....	11
3.6	Step 6: eReceipt Issuance.....	12
4	Roles and participants.....	12
4.1	Scenario roles and participants.....	12
4.2	Additional roles and partners	12
4.3	Requirements.....	13
5	Attestations	14
5.1	Introduction	14
5.2	Attestations to be provided by Authentic sources, other than the company.....	14
5.3	Created attestations in the scenario by the companys' EBW.....	14
	Annex 1 – Requirements for scenario roles.....	15
	Annex 2 - EN 16931-1:2026 Revision Analysis	17
	E.1 Standard Versioning.....	17
	E.2 Key Changes in the 2026 Revision	17
	E.3 Syntax Binding Status.....	17
	E.4 CEN/TS 16931-8:2024 — The eReceipt Standard.....	18
	E.5 Migration and Backward Compatibility	18

<i>E.6 Change Pressures Not Yet Addressed — Future Roadmap.....</i>	<i>18</i>
ANNEXE 3 _ illustration of the workflow to issue an eReceipt.....	20

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 1.1., as part of use case PA4 in work package 3 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

Scenario 1.1 (PA4) demonstrate how the European Digital Identity Wallet (EUDI Wallet) and the European Business Wallet (EBW) can transform Business-to-Business (B2B) payment processes across the EU by enabling secure, verified payment confirmation across two distinct transaction workflows: eInvoicing and eReceipt.

The eReceipt attestation is a standardized digital attestation that replaces the paper receipt and reliably links each payment transaction to a proof that can be exploited by banks, merchants and third parties (accounting, tax, expense management).

- ✓ It normalizes a common set of transactional data (amounts, VAT, merchant, point of sale, means of payment, products, etc.) to facilitate interoperability between PSPs, wallets, banks and control ecosystems.

The eReceipt is designed as a “verifiable credential” compliant with the European EUDI framework, with an explicit assurance level, which enables its use in regulated journeys or those with high compliance requirements. It can be enriched for specific use cases such as mobility, travel or B2B (for example expense management, automatic categorization, CO₂ data), paving the way for new value-added services for banking customers

This scenarios addresses businesses of all sizes—large enterprises, SMEs, and sole traders—engaging in cross-border digital payment transactions:

This scenario aims to demonstrate how the eReceipt can be seamlessly issued and distributed for a card payment with deferred invoice, ensuring that the digital receipt remains a trustworthy, standardized proof of the underlying transaction for banks, merchants and third parties. It shows end-to-end how the payment authorization, clearing and eReceipt issuance are linked, and how the attestation can be reused in banking or merchant services (disputes, expenses, loyalty, compliance).

The scenario is designed to reflect the complex reality of B2B payment operations faced by businesses and public authorities today. Current payment processes involve manual verification, fragmented identity checks, and reconciliation challenges that consume significant operational resources and create friction in cross-border commerce.

The scenario covers an online purchase paid by corporate card (debit or credit) where the invoice issuing is deferred (end-of-month or later), from authorization through to clearing and eReceipt generation and delivery to the customer's wallet or banking app. It includes the data exchanged between the merchant, the PSP/acquirer, the issuer/bank and the eReceipt issuer, as well as the verification of the attestation by relying parties (e.g. bank app, expense tool). Out of scope are the detailed risk-management and scoring algorithms, the full lifecycle of chargebacks and refunds,

This scenario is key because card with deferred invoice is a dominant use case in many markets, making it a high-impact playground to prove the value of standardized eReceipts at scale. It shows concretely how the eReceipt can reduce friction and costs for merchants (less disputes on amounts and VAT, easier after-sales) while enabling banks to offer richer services around card transactions (clear purchase history, expenses, budgeting, loyalty) on top of a reliable, interoperable data layer. It also demonstrates that the eReceipt model is compatible with complex settlement patterns (deferred, batch, partial, multi-installment), which is critical for regulatory acceptance and for adoption by large issuers and acquirers.

The scenario is based on the following documentation:

- WeBuild Architecture & Integration Blueprint Reference Document
[WE BUILD — Architecture & Integration Blueprint \(D4.1\)](#)
- PA4 stock taking document
<https://portal.webuildconsortium.eu/group/pa4-business-payments/files?mid=5857&fid%5B0%5D=236&fid%5B1%5D=237&fid%5B2%5D=4212>
- PA2 stock taking document
<https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=5920&fid%5B0%5D=201&fid%5B1%5D=202&fid%5B2%5D=4208>
- European Business Wallet Regulation (draft)
[EUR-Lex - 52025PC0838 - EN - EUR-Lex](#)
- EUDI Wallet Architecture and Reference Framework (ARF) – version 2.9
[European Digital Identity](#)
- Domain-specific standards for eInvoicing and payment interoperability (Peppol BIS Billing 3.0, ISO 20022, EN 16931, HEROJson)

2 Scenario specification

2.1 Introduction

This scenario 1.1 (PA4) covers retail-style purchases online—where the merchant lists products and provides order information. Payment transactions are highly secure, standardized, and regulated. Individual Business card is issued to EUDI-wallet. In the initiation

of payment SCA is performed and eReceipt is delivered after successfully completed transaction.

Scenario uses BU1 KYC/KYS-attestations for registering buyer and PA2 card payment flow concerning Strong Customer Authentication. In this scenario PA4 will create payment receipt and deliver it to EBW-wallet.

Key Characteristics:

- Timeline: Payment completes in seconds (vs. days/months for eInvoices)
- Relationship: Merchant does not know the customer (no KYC/KYB); merchant validation is performed by acquirers, payment facilitators/aggregators, and card rails (domestic or international card schemes)
- Typical B2B Use Case: Expense management scenarios (ferry tickets, parking, etc.)
- SME Reality: Personal cards are used extensively for business purchases due to better payment terms

2.2 Scenario pre-conditions

To ensure the successful execution of this scenario, the following preconditions must be met:

Before the main workflow can start, each actor must already be provisioned with the right credentials and connections. The bullets below list the one-time setup steps that must have happened *before* the eInvoice is sent; they are not part of PA4's runtime flow, but PA4 will not execute correctly without them.

Seller pre-requisites

- The Business Register has issued an EBWOID to the Seller, provisioning the Seller's Business Wallet.
- The Seller is connected to an Invoice Processor (its own internal system or equivalent e-invoicing infrastructure) through which the eInvoice can be sent.

Category	Wallet	Attestation	Details
Identity Setup	EUDI Wallet	Personal Identification Data (PID)	Individual identity attestation stored in EUDI Wallet
Business & Banking Setup	EU Business Wallet	EU Business Wallet Organizational ID (EUBWOID)	Business registration attestation stored in EU Business Wallet
	EU Business Wallet	EU Company Certificate (EUCC)	Verified legal entity attestation
	EU Business Wallet	IBAN Attestation	Issued following bank account onboarding via PA3 Scenario 1 and/or 3
Operational Readiness	EU Business Wallet	Invoicing Capability	Ability to issue structured invoices (Peppol BIS Billing 3.0, EN 16931)
	E-commerce platform		
	External system	Bank integration	
	External System	Invoice Network Integration	Peppol Access Point or equivalent e-invoicing infrastructure

Buyer pre-requisites

- The Authorised Person's EUDI Wallet is in the "Active" state (see §2.2 for what this entails and why it is out of scope for PA4).
- The Business Register has issued an EBWOID to the Buyer, provisioning the Buyer's Business Wallet.
- A Bank Wallet has been defined for the Buyer at its Home Bank.
- The Buyer is connected to an Invoice Processor (its own internal system or equivalent e-invoicing infrastructure) so that incoming eInvoices land in the Business Wallet.
- The Buyer is connected to a Payment Processor (its own internal system or an external PSP) so that card payments can be initiated.

Category	Wallet	Attestation	Details
Identity Setup	EUDI Wallet	Personal Identification Data (PID)	Individual identity attestation stored in EUDI Wallet
Business & Banking Setup	EU Business Wallet	EU Business Wallet Organizational ID (EUBWOID)	Organizational identity attestation stored in EU Business Wallet
	EU Business Wallet	EU Company Certificate (EUCC)	Verified legal entity attestation
	EU Business Wallet	IBAN Attestation	Issued following bank account onboarding via PA3 Scenario 1
	EBW	EBW linkage with bank for PoA	
	EBW	Capability to receive and handle eReceipt	
Supplier Relationship	EU Business Wallet	Supplier Onboarding (KYS)	Completed via BU1 Know Your Supplier process – establishes trusted supplier relationship and validates seller credentials Relevant for Scenario 1.1

2.3 Scenario main flow

The flow is broken into six steps that always run in the same order:

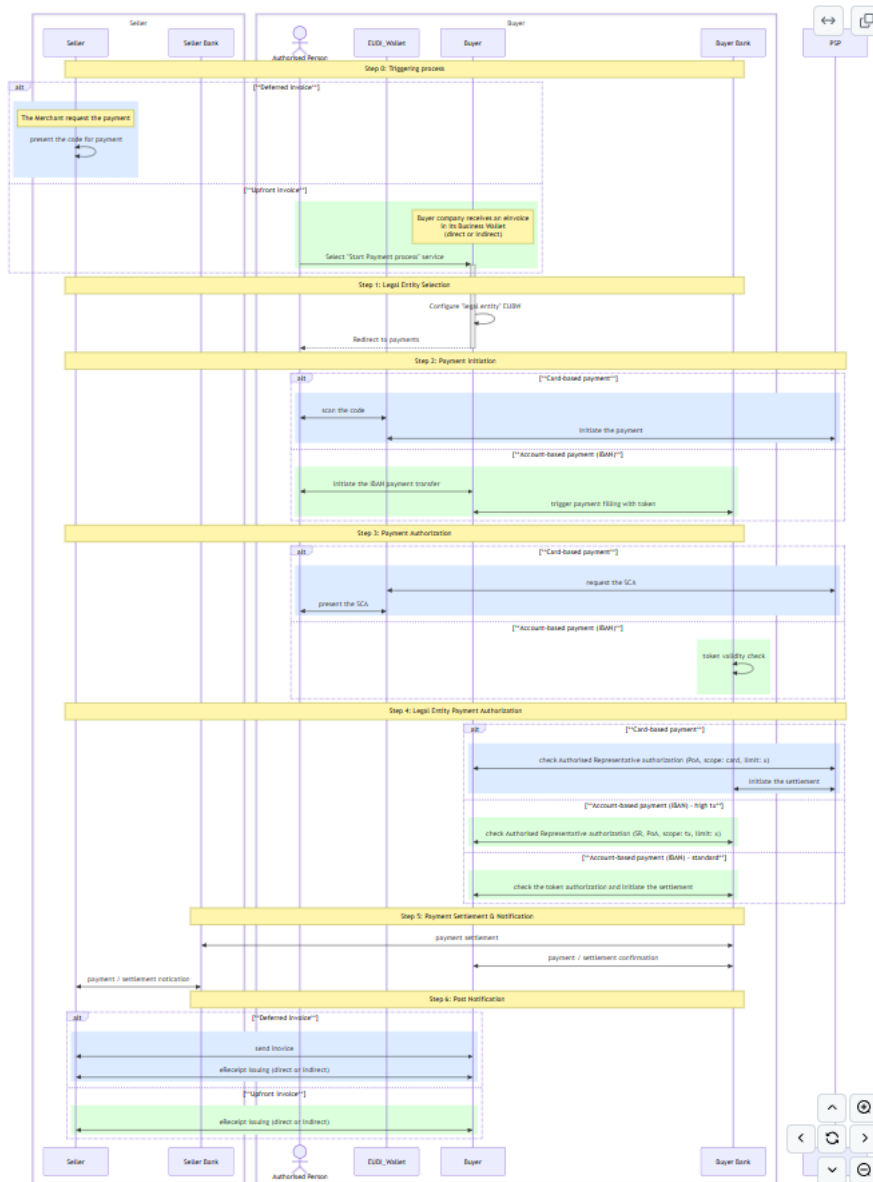
- (1) pick the legal entity
- (2) initiate the payment
- (3) authorise the person (SCA)
- (4) authorise the legal entity (SR/PoA)
- (5) settle
- (6) issue the eReceipt.

Illustrations are presented in annexe.

[wp3-technology-standards/sequence-diagrams/PA4](https://www.w3.org/2021/07/wp3-technology-standards/sequence-diagrams/PA4) at main · [webuild-consortium/wp3-technology-standards](https://github.com/webuild-consortium/wp3-technology-standards)

Note: Color legend:

- Blue – Deferred Invoice
- Green – Upfront Invoice
- White – Applicable to both scenarios



2.4 Challenges and barriers

As outlined in the specification document, this use case is based on a set of assumptions that allow coverage of the majority of relevant scenarios. However, special or edge cases would need to be revisited and addressed when designing a production-grade implementation.

Key challenges that this use case highlights include the need for clear decisions and technical specifications regarding:

- Wallet discovery mechanisms
- Mutual authentication between participating parties
- Automation capabilities related to the European Business Wallet (EBW)
- The trust infrastructure, particularly for (Q)EAAs and certificates
- The core verification process, including which checks will be performed within the WE BUILD framework to ensure that attestations are authentic, valid, and trustworthy

2.5 Working Assumptions

The MVP cannot exercise the full target architecture, so we pin several variables to known values. Each subsection below states what we assume to be true for one perspective (Seller, Buyer, Authorised Representative, and the two wallets), so reviewers can quickly find the assumptions that affect their area. If any of these assumptions fails in practice, the corresponding step in §8 will not behave as described.

2.5.1 Seller (Holder)

- Holds an active EBW with only the minimum set of attestations required to execute PA4.
- Not required to complete Home-Bank onboarding (PA3) or KYS onboarding (BU1 – KYS).
- Classified exclusively as low- or medium-risk.

2.5.2 Buyer (Relying Party)

- Holds an active EBW with only the minimum set of attestations required to execute PA4.
- Not required to complete Home-Bank onboarding (PA3) or KYC onboarding (BU1 – KYC).
- Onboarding of the Authorised is performed as part of end-customer onboarding (not as a separate business-representative onboarding under PA2).
- Business Wallet is assumed to contain valid Signatory Rights (SR) attestations together with the corresponding PoA for the Authorised Representative.

2.5.3 Authorised Person

- Holds a valid EUDI Wallet containing a PID credential.
- Holds the SCA attestation in the wallet.

- Validation of the company's list of Authorised Persons (SR) is out of scope for the MVP.
- Performs SCA using possession of the wallet device combined with PIN or biometric authentication.

2.5.4 Holder Business Wallet

- Automatic flow
- Mutual authentication is enabled by default; no TLOL or device-binding checks are applied.
- The buyer wallet is pre-authorised to both present and receive attestations; no additional configuration is supported in the MVP.
- The Business Wallet accepts credential offers automatically when an active corporate authorisation session is already established.
- Manual flow
- Mutual authentication is reduced to a visual verification step.
- Authorization is reduced to a visual check and manual approval.

2.5.5 Relying-Party Business Wallet

- Attestation verification for each attestation is limited to:
- Cryptographic validation (Section 4.2.1).
- Issuer identification against an internal trusted list (Sections 4.2.2 – 4.3.3).

2.5.6 General

- The payment process is executed sequentially in a single-user flow.
- The eInvoice is assumed to have already been received in the Business Wallet.
- The process concludes with the issuance of the eReceipt attestation into the Business Wallet.
- No attestation is issued to the Authorised Person's EUDI Wallet.

3 Detailed scenario flow

The diagram below is the single picture to remember. Read it top-to-bottom: the eInvoice arrives, the Authorised Person starts the process at the Bank, and each subsequent block (Steps 1–6) lines up with one of the detail subsections that follow. alt ... else ... end blocks represent the card-vs-IBAN branches.

3.1 Step 1: Legal Entity Selection

The Authorised Person may represent more than one company, so the first thing the Bank needs to know is on whose behalf this payment is happening. Nothing in the rest of the flow makes sense until this binding is made.

Goal: Identify which legal entity the Authorised Person is acting on behalf of and start the payment process.

Pre-condition: eInvoice present in Buyer's EBW; Authorised Person authenticated to the Bank channel.

Actors: Authorised Person, Bank.

Post-condition: Bank session bound to the selected legal entity.

Errors / fallbacks: Legal-entity discovery fails → Authorised Person is prompted to re-select; session is not bound.

3.2 Step 2: Payment Initiation

Here the workflow forks for the first time, depending on the payment rail chosen by the Authorised Person. The card path involves the EUDI Wallet and the PSP; the IBAN path stays inside Buyer ↔ Bank. After this step the rails do not re-merge until settlement.

Goal: Initiate payment over the chosen rail.

Branches:

Card: Authorised Person scans a code with EUDI Wallet → EUDI Wallet initiates payment with PSP.

Post-condition: A pending payment instruction exists at PSP or Bank.

Errors / fallbacks: Code scan fails (card) or token generation fails (IBAN) → process aborts before authorization.

3.3 Step 3: Payment Authorization

This step answers the question "is the right person approving this payment?". For card payments, that means a full SCA prompt against the EUDI Wallet; for standard IBAN payments, the Bank's pre-issued token is treated as a proxy for that approval, so no SCA is shown to the user.

Goal: Authenticate the Authorised Person for the payment.

Branches:

Card: PSP requests SCA from EUDI Wallet; Authorised Person presents SCA (PIN or biometric).

Errors / fallbacks: SCA failure → payment is rejected; token invalid → IBAN flow aborts.

3.4 Step 4: Legal Entity Payment Authorization

Step 3 proved who is approving; Step 4 proves they are allowed to approve on behalf of the company, for this rail and this amount. This is where Signatory Rights and Power of Attorney attestations are checked. A high-value IBAN transaction triggers the strictest check (SR + PoA with a transaction-level limit).

Goal: Confirm the Authorised Person has authority for the legal entity to execute this payment.

Branches:

Card: PSP verifies Authorised Person authorization against Buyer (PoA scope: card, limit: x), then asks Bank to settle.

Errors / fallbacks: Missing or insufficient SR/PoA → settlement is not initiated.

3.5 Step 5: Payment Settlement

With both the person and the company authorised, the Bank performs the actual movement of funds. From the user's perspective this step is largely invisible; they will only see the resulting confirmation.

Goal: Move funds and notify Buyer.

Flow: Bank performs settlement internally and confirms to Buyer.

Post-condition: Payment is settled and Buyer holds a settlement confirmation.

3.6 Step 6: eReceipt Issuance

The eReceipt is the persistent, verifiable proof that the invoice was paid, and its delivery to the Buyer's EBW is the formal end of the workflow. Note that the receipt is a company-level artefact: it lands in the Business Wallet, not in the Authorised Person's EUDI Wallet.

Goal: Deliver an eReceipt attestation to the Buyer's EBW.

Flow: Buyer obtains the eReceipt from Seller (direct or indirect).

Post-condition: eReceipt attestation is stored in Buyer's EBW. No attestation is issued to the Authorised Person's EUDI Wallet.

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
Buyer 1 (Relying Party for eReceipt) User of wallet	Sole Trader (via Bootes Booking Platform)	Finland
Buyer 2 (Relying Party for eReceipt) User of wallet	Travel Agent (via Bootes Booking Platform)	Greece
Seller (Authentic source for eReceipt) User of wallet	Fast Ferries	Greece
Wallet provider (for buyer 1 – sole trader)	IGrant.io (EUDIW)	Sweden
Wallet provider (for buyer 2 – Travel Agent)	IGrant.io (EBW)	Sweden
Wallet provider (for seller)	Procivis (EBW)	Switzerland
Intermediary for wallet integration (buyer & seller)	UAegean	Greece
Intermediary for PSP acquiring	Worldline	France or Germany or Greece
Intermediary (eReceipt)	ReceiptHero Oy	Finland
Card Attestation	OP Bank	Finland

Authentic sources in this use case are needed for companies and financial institutions. The later require for the MVP flow an EBWID and EUCC, therefore less data requirements arise for authentic sources covering this.

4.2 Additional roles and partners

Current working assumption is that we achieve conformance within the use case. And that any wallet provided within the country can be used across borders. So no specific matching of countries is done here.

4.3 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.

Overview over the attestations and required attribute are here

[webuild-attestation-rulebooks-catalog/rulebooks at main · webuild-consortium/webuild-attestation-rulebooks-catalog](#)

5.2 Attestations to be provided by Authentic sources, other than the company

...

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	Requirements
PID	Personal Identification Data	PA1 / Member state PID Provider	eIDAS 2.0 Level of Assurance High
EUBWID	EU Business Wallet Organisational ID	PA1 / EBW Provider	Issued upon EBW activation; links natural person to legal entity
EUCC	EU Company Certificate	PA1 / National business register	Authentic source: national commercial register (PRH, Handelsregister, Bolagsverket)
IBAN Attestation	Bank account ownership confirmation	PA3 Scenario 1 and/or 3	Issued by account-holding bank following onboarding. Required for SEPA payment path (Scenario 1.1).
SCA Attestation	Strong Customer Authentication proof	PA2 B1 / PA3 / Issuing bank	PSD2/PSR compliant SCA. Card path: EMV chip+PIN or EUDI Wallet SCA. IBAN path: bank SCA.
KYS (Supplier Onboarding)	Know Your Supplier — trusted supplier relationship	BU1 / Buyer EBW	Completed via BU1 KYS process. Scenario 1.1 only (not required for 1.2 expense management).

5.3 Created attestations in the scenario by the companys' EBW

EAA – Attestation issued by the company out of the Business Wallet

Attestation name	Short description	Issuer	For Countries	Applicable domain standards
DS-011 eReceipt (vReceipt)	Structured proof of purchase — items, VAT, merchant identity, payment verification	Merchant or PSP/Acquirer, via eReceipt Intermediary (technical issuer)	FI, DE, SE	SD-JWT VC (EWC RFC011), HeroJSON field names, CEN/TS 16931-8:2024, OIDC4VCI (RFC001), OIDC4VP (RFC002)
DS-012 Payment Attestation	Bank-issued payment event confirmation — amount, parties, rail-specific verification data	Issuing Bank (card) / Account-holding Bank (SEPA)	FI, DE	SD-JWT VC, ISO 20022 (pain.001, camt.054), EMV Specifications, EPC125-05 SCT Rulebook
DS-013 eReceipt Routing Credential	Employer-issued routing credential — maps card/IBAN tokens to Business Wallet endpoint (early draft)	Employer (via EBW or HR system)	FI, DE, SE	SD-JWT VC, OIDC4VCI (RFC001), OIDC4VP (RFC002), ARF 1.6
IPC (Invoice Payment Confirmation)	Payment confirmation for structured e-invoice — links Peppol invoice to SEPA payment	Account-holding Bank	FI, DE	SD-JWT VC, Peppol BIS Billing 3.0, EN 16931-1, ISO 20022

Annex 1 – Requirements for scenario roles

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

- **High-Level Requirements:**

For banks, the impact is concentrated in digital channels and verification logic, not in core banking. They will need to adapt their mobile/web channels to display an additional “digital receipt” element on card transactions in the pilot perimeter, and implement lightweight verification and matching to their internal transaction records. Operational units (customer service, disputes, compliance) should be informed and involved in evaluating how eReceipts change the handling of claims and controls, without changing formal regulatory processes during the pilot.

- **What Participants Need to Do (“Shopping bag”):**

Merchants (or seller or authentic source for eReceipt):

Be able to provide the necessary transactional data to build an eReceipt that meets the rulebook (including VAT, line items where applicable).

Agree on a pilot perimeter (websites, card ranges, types of transactions) and ensure staff and support teams understand that eReceipts are being tested.

PSPs / Acquirers / eReceipt issuers:

Implement the generation of eReceipts from card transaction data, in compliance with the rulebook, and expose them via standard interfaces to wallets / banking apps.

Maintain a minimal status and lifecycle management for the eReceipts (issued, revoked, corrected) for the duration of the pilot.

Banks / Issuers / Relying parties:

Implement the consumption of eReceipts in at least one digital channel (e.g. a test version of the mobile banking app, a web portal, or a wallet) with a simple UX linking a card transaction to its eReceipt.

Implement a basic verification mechanism (trust anchor configuration, status check, consistency checks with card transaction), at least in a pilot environment.

Nominate business and operational contacts to capture feedback (customer service, disputes teams, compliance, product).

Wallet providers / Apps (where relevant):

Integrate the receipt of eReceipts, their storage and display, and support a simple “share/present for verification” flow in line with the rulebook profiles.

- **Implementation Clarity / Impact:**

For merchants, the impact is mainly on data quality and integration with the PSP or eReceipt issuer: ensuring that existing POS/cash register systems can provide the right level of detail to build compliant eReceipts. Process impacts are limited: receipts remain issued as today, with eReceipts added on top for the pilot perimeter.

Annex 2 - EN 16931-1:2026 Revision Analysis

This section provides a strategic analysis of the EN 16931 standard revision and its implications for the PA4 eReceipt and eInvoice attestations.

E.1 Standard Versioning

Current status: **CEN approved the revised EN 16931-1 on 13 February 2026** (formally published as EN 16931-1:2026). Definitive Text available since 18 March 2026. National Standard Bodies must publish by 31 May 2026.

Previous version: EN 16931-1:2017 was the original B2G e-invoicing standard mandated by Directive 2014/55/EU. The 2026 revision is **not backward compatible** — invoices valid under 2017 will not pass 2026 validation.

E.2 Key Changes in the 2026 Revision

ViDA-Driven Requirements

- IBAN fields: expanded payment information to support Digital Reporting Requirements (DRR) from 1 July 2030
- Margin scheme support: national VAT special schemes now standardised
- Goods/services indicator: new field distinguishing product types for CTC reporting
- Triangulation indicators: support for VAT simplification in three-party chains

B2B Extensions

- Multiple order references per invoice: single invoice can reference several purchase orders
- Multiple buyer identifiers: supports the payer ≠ buyer dynamic central to PA4 Scenario 1.2
- XML attachments: structured data can be embedded within the invoice
- Advanced payment terms: early payment discounts, late-payment charges
- New VAT codes and exemption reason codification

Invoice Management

- Issuance timestamp: standardised field for exact invoice creation time (relevant for real-time reporting)
- Corrective invoice sequencing: formalised handling of credit notes and corrections

E.3 Syntax Binding Status

Binding	Status (April 2026)	Implication
UBL 2.5	TS draft accepted internally by TC 434. Formal vote scheduled July 2026.	Peppol BIS 4.0 will be built on this. Cannot build conformant implementations until finalised.
UN/CEFACT CII D25A	TS draft accepted. Same July 2026 vote timeline.	XRechnung 4.0 (Germany) will align. Critical for DE pilot partners.
Peppol BIS 4.0	Under development by OpenPeppol. Merges BIS 3.0 + PINT into unified standard.	PA4 Scenario 1.1 eInvoice path depends on this. Timeline not yet confirmed.

E.4 CEN/TS 16931-8:2024 — The eReceipt Standard

CEN/TS 16931-8:2024 (published October 2024) defines the *semantic data model for e-receipts and simplified electronic invoices*. This is the CEN-level standard that directly corresponds to DS-011 eReceipt content.

The standard establishes a semantic model including essential information elements for legal (including fiscal) compliance and cross-border interoperability. It covers both B2B expense management and B2C consumer receipts. The 110-page specification provides the formal basis for the HeroJSON field names used in DS-011.

Key alignment: DS-011 v2.2 attributes map directly to CEN/TS 16931-8 business terms. The VAT codes in DS-011 (vats[].VATCode) use the EN 16931-1 category codes (S, Z, E, etc.). This alignment ensures that eReceipts are interoperable with eInvoice infrastructure.

E.5 Migration and Backward Compatibility

The 2026 revision is explicitly **not backward compatible** with EN 16931-1:2017. This has significant implications:

- ERP systems, access points, and matching workflows will all need updates
- Peppol BIS 4.0 will be the unified standard — current BIS 3.0 implementations must migrate
- Denmark has announced Nemhandel BIS 4 with a 2029 migration timeline, cancelling OIOUBL 3.0
- Germany's XRechnung 4.0 will align with EN 16931-1:2026 — critical for DATEV/Bosch pilot path

For PA4 pilot: The pilot should be designed to work with both EN 16931-1:2017 (current production) and EN 16931-1:2026 (target). DS-011 and IPC attestation schemas should support both versions during the transition period (estimated through ViDA 2030 go-live).

E.6 Change Pressures Not Yet Addressed — Future Roadmap

The following change pressures are visible but not yet incorporated into EN 16931 or the PA4 specification. They represent potential future roadmap items.

Pressure	Description	PA4 Relevance
PSD2/PSR vs. eIDAS2 SCA gap	PSD2 SCA requires dynamic linking; eIDAS2 Strong User Authentication (SUA) does not. PSPs unsure which to implement. PSR (replacing PSD2) expected formal adoption mid-2026, effective 2028.	Directly affects PA4 Block 3 (SCA). MVP uses EMV chip+PIN (bypasses the conflict). EUDI Wallet SCA path blocked until PSR clarifies.
CSRD Scope 3 emissions data	Corporate Sustainability Reporting Directive requires Scope 3 (supply chain) emissions data from 2026. Structured receipts could carry CO2 data per product line.	DS-011 already includes journey{} object for travel emissions. Future extension: products[].carbonFootprint field. Not in MVP but architecturally prepared.
Real-time DRR reporting	ViDA Pillar 1 mandates real-time Digital Reporting Requirements from 1 July 2030. Requires invoice data transmission to tax authorities within 5 days of issuance.	eReceipts with itemised VAT (DS-011) are DRR-ready. Could serve as automated tax reporting input. Future extension beyond expense management.
Agentic commerce / AI-initiated payments	PA2 Risk & Fraud WG (Q4) identifies AI-initiated payments as emerging fraud/liability concern. No regulatory framework yet.	Future PA4 use case: AI-driven expense submission and approval. ReceiptHero's structured data enables automated policy checks. Liability model undefined.

Payment Wallets WG	New PA2 working group (PayPal leading, kickoff June 2026) analysing EUDI Wallet impact on existing payment wallets (Apple Pay, Google Pay, PayPal).	eReceipt delivery channel. If payment wallets become EUDI Wallet intermediaries, the receipt delivery question becomes: which wallet receives the receipt? DS-013 routing solves this. ApplePay & GooglePay supported in production.
EN 16931 Part 8 → full EN promotion	CEN/TS 16931-8 is currently a Technical Specification (TS), not a full European Norm (EN). If e-receipts become mandated (like e-invoicing via Directive 2014/55/EU), promotion to EN may follow.	Would create a legal mandate for structured receipts, analogous to B2G e-invoicing. Strongest possible regulatory tailwind for PA4 eReceipt adoption.
Cross-border VAT refund automation	Current VAT refund for cross-border business purchases (Directive 2008/9/EC) requires manual documentation. Structured eReceipts could automate the claim.	DS-011 contains all required data: merchant VAT ID, itemised VAT amounts per rate, payment proof. Future integration with Member State refund portals.

ANNEXE 3 _ illustration of the workflow to issue an eReceipt

Figure 1 Pre-condition: KYC/KYS process

Figure 2 Common: card or invoice

Figure 3 Scenario 1.1. SCA of payment

Figure 4 Scenario 1.1. Issuance of eReceipt of card payment

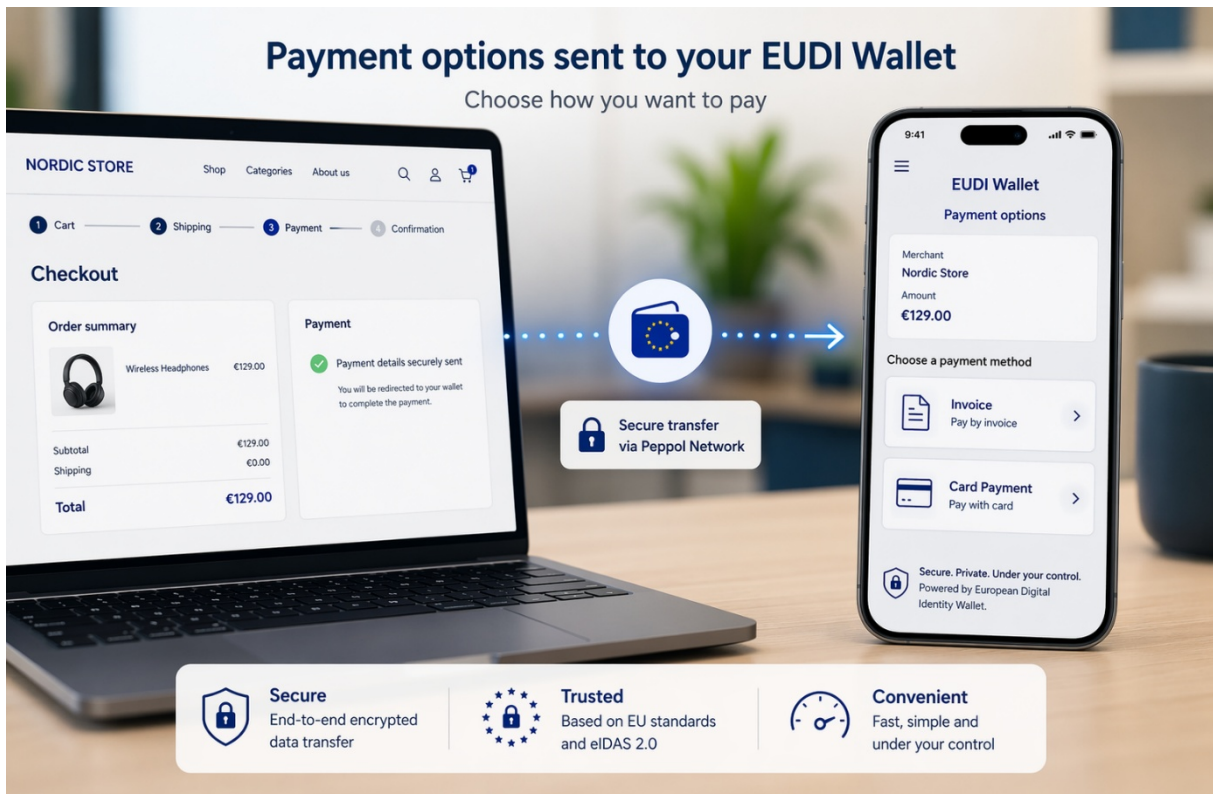
Figure 5 Scenario 1.2. approval of invoice

Figure 6 Scenario 1.2. Payment reception verification delivered to buyer



Payment options sent to your EUDI Wallet

Choose how you want to pay





Secure
End-to-end encrypted
data transfer



Trusted
Based on EU standards
and eIDAS 2.0



Convenient
Fast, simple and
under your control

Card payment approved in your European Digital Identity (EUDI) Wallet

A secure and convenient way to pay online



1. Choose card payment at checkout

2. Select your card in EUDI-wallet

3. Authenticate with fingerprint or PIN code

4. Payment approved securely



Secure
Strong authentication
keeps your payments safe



Privacy first
Your data is protected
and under your control



Convenient
Fast and easy payments
wherever you shop



European solution
Built on EU standards
for trust and interoperability

Receipts in your EUDI Wallet and accounting software

The same receipt – securely stored and automatically available in your accounting

The diagram illustrates the secure sharing and syncing of a receipt between an EUDI Wallet and Accounting software. A smartphone displays the EUDI Wallet interface, showing a receipt from Nordic Store for Wireless Headphones. A laptop displays the Accounting software interface, showing the same receipt. A cloud icon with a checkmark and arrows indicates the secure sharing and syncing process.

EUDI Wallet

Accounting software

Securely shared and synced

The receipt is securely delivered via the Peppol Network and automatically available in your accounting system.

- Reliable**
Data delivered via Peppol Network
- Secure**
End-to-end encrypted and compliant
- Efficient**
No manual entry – saves time and reduces errors

Peppol e-invoice – Verified and ready for approval

Secure, compliant and fully traceable

The diagram illustrates the verification and approval process for a Peppol e-invoice. It shows the invoice details, the automatic verification process, and the final approval status.

INVOICE

Invoice number: INV-2024-0515
Issue date: 15 May 2024
Due date: 29 May 2024

Seller: Nordic Solutions Oy
Business ID (VAT): FI12345678
Address: Mannerheimintie 12 B, 00100 Helsinki, Finland

Buyer: Acme Corporation Oy
Business ID (VAT): FI87654321
Address: Porkkalankatu 1, 00180 Helsinki, Finland

Item	Description	Quantity	Unit price	VAT %	Amount
1	Wireless Headphones	10 pcs	129,00	24%	1 290,00
Subtotal					1 290,00
VAT 24%					309,60
Total EUR					1 599,60

Payment details: IBAN: FI12 3456 7890 1234 56, BIC: NDEAFIHH, Bank: Nordea Bank Abp

Other information: Peppol format: UBL 2.1, Peppol ID (Seller): 0192:FI12345678, Peppol ID (Buyer): 0192:FI87654321, Profile ID: urn:fdc:peppol.eu:2017:poacc:billing:01:1.0, Customization ID: b3f2a6d9-7c1e-4b09-8e3e-0b5f9e8c1d2a, Transmission ID: b3f2a6d9-7c1e-4b09-8e3e-0b5f9e8c1d2a

Automatic verification

- IBAN verified: Nordea Bank Abp
- VAT number verified: FI12345678
- Peppol format valid: UBL 2.1
- Invoice integrity: No changes detected
- Seller identity verified: Nordic Solutions Oy

All checks passed. Ready for approval.

Business Wallet Invoice approval

From: Nordic Solutions Oy
Invoice number: INV-2024-0515
Amount: 1 599,60 EUR
Due date: 29 May 2024

- IBAN: FI12 3456 7890 1234 56
- VAT number (Seller): FI12345678
- Peppol validation: All checks passed

This invoice is valid. You can approve it for payment.

Approve invoice

Reject invoice

- Secure**
End-to-end encrypted data exchange
- Compliant**
Based on EU standards and eIDAS 2.0
- Efficient**
Faster processing, fewer errors
- Sustainable**
Paperless and better for the environment

Invoice paid – Reception verified

The invoice is paid and successfully received by the buyer

✓ PAID

✓ Reception verified



INVOICE

Invoice number INV-2024-0515
Issue date 15 May 2024
Due date 29 May 2024



Peppol ID (Seller)
0192:FI12345678
Peppol ID (Buyer)
0192:FI87654321

Seller
Nordic Solutions Oy
Business ID (VAT)
FI12345678 ✓
Address
Mannerheimintie 12 B
00100 Helsinki, Finland

Buyer
Acme Corporation Oy
Business ID (VAT)
FI87654321 ✓
Address
Porkkalankatu 1
00180 Helsinki, Finland

Description	Quantity	Unit price	VAT %	Amount
Consulting services	10	120,00	24%	1 200,00
Software license	1	800,00	24%	800,00
			Subtotal	2 000,00
			VAT 24%	480,00
			Total EUR	2 480,00

Payment details

IBAN FI12 3456 7890 1234 56 ✓
BIC NDEAFIHH
Bank Nordea Bank Abp

Additional information

Invoice format UBL 2.1
Customization ID urn:fdc:peppol.eu:2017:poacc:billing:01:1.0
Profile ID urn:fdc:peppol.eu:2017:poacc:bis-invoice:3.0
Transmission ID b3f2a6d9-7c1e-4b09-8e3e-0b5f9e8c1d2a

✓ This invoice was received via the Peppol Network.
This invoice has been paid and the reception has been verified by the buyer.

Status

- ✓ **Paid**
Payment completed on 29 May 2024
- ✓ **Reception verified**
Verified by the buyer on 29 May 2024

What this means

- ✓ **Delivered**
Invoice successfully delivered via the Peppol Network
- ✓ **Paid**
Payment has been received
- ✓ **Reception verified**
Buyer has confirmed receipt of the invoice

Benefits

- ✓ **Secure & compliant**
Meets EU standards and regulations
- ✓ **Efficient**
No manual handling, real-time status
- ✓ **Sustainable**
Paperless process

WE BUILD consortium

Specification PA4 Scenario 1.2 _ IBAN payment _ upfront invoice

WP3 – PA4 (Corporate Payments)

Date : 20.June.2026
Version : 1.0
Status : FINAL

Index

1 Introduction4

- 1.1 Objectives of this document4*
- 1.2 Scenario introduction4*

2 Scenario specification5

- 2.1 Introduction5*
- 2.2 Scenario pre-conditions6*
- 2.3 Scenario main flow7*
- 2.4 Challenges and barriers9*
- 2.5 Working Assumptions9*
 - 2.5.1 Seller (Holder)9*
 - 2.5.2 Buyer (Relying Party)9*
 - 2.5.3 Authorised Person10*
 - 2.5.4 Holder Business Wallet10*
 - 2.5.5 Relying-Party Business Wallet10*
 - 2.5.6 General10*

3 Detailed scenario flow10

- 3.1 Step 1: Legal Entity Selection10*
- 3.2 Step 2: Payment Initiation11*
- 3.3 Step 3: Payment Authorization11*
- 3.4 Step 4: Legal Entity Payment Authorization11*
- 3.5 Step 5: Payment Settlement12*
- 3.6 Step 6: eReceipt Issuance12*

4 Roles and participants12

- 4.1 Scenario roles and participants12*
- 4.2 Additional roles and partners12*
- 4.3 Requirements13*

5 Attestations14

- 5.1 Introduction14*
- 5.2 Attestations to be provided by Authentic sources, other than the company14*
- 5.3 Created attestations in the scenario by the companys' EBW14*

Annex 1 – Requirements for scenario roles15

Annex 2 - EN 16931-1:2026 Revision Analysis17

- E.1 Standard Versioning17*
- E.2 Key Changes in the 2026 Revision17*
- E.3 Syntax Binding Status17*
- E.4 CEN/TS 16931-8:2024 — The eReceipt Standard18*
- E.5 Migration and Backward Compatibility18*

*E.6 Change Pressures Not Yet Addressed — Future Roadmap*¹⁸

ANNEXE 3 _ illustration of the workflow to issue an eReceipt²⁰

1 Introduction

1.1 Objectives of this document

This document describes the details of scenario 1.2 – IBAN payment upfront invoice., as part of use case PA4 in work package 3 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

Scenario 1.2 (PA4) demonstrate how the European Digital Identity Wallet (EUDI Wallet) and the European Business Wallet (EBW) can transform Business-to-Business (B2B) payment processes with IBAN across the EU by enabling secure, verified payment confirmation across two distinct transaction workflows: eInvoicing and eReceipt.

The eReceipt attestation is a standardized digital attestation that replaces the paper receipt and reliably links each payment transaction to a proof that can be exploited by banks, merchants and third parties (accounting, tax, expense management).

- ✓ It normalizes a common set of transactional data (amounts, VAT, merchant, point of sale, means of payment, products, etc.) to facilitate interoperability between PSPs, wallets, banks and control ecosystems.

The eReceipt is designed as a “verifiable credential” compliant with the European EUDI framework, with an explicit assurance level, which enables its use in regulated journeys or those with high compliance requirements. It can be enriched for specific use cases such as mobility, travel or B2B (for example expense management, automatic categorization, CO₂ data), paving the way for new value-added services for banking customers.

This scenarios addresses businesses of all sizes—large enterprises, SMEs, and sole traders—engaging in cross-border digital payment transactions:

This scenario aims to demonstrate how an eReceipt attestation can be issued and delivered in the context of a payment by IBAN based on an upfront invoice (e.g. SEPA credit transfer), ensuring a robust digital proof of the underlying commercial transaction. It shows end-to-end how the invoice, the payment order and the eReceipt are linked, and how this attestation can be relied upon by banks, merchants and third parties for reconciliation, compliance and value-added services

The scenario is designed to reflect the complex reality of B2B payment operations faced by businesses and public authorities today. Current payment processes involve manual verification, fragmented identity checks, and reconciliation challenges that consume significant operational resources and create friction in cross-border commerce.

The scenario covers a purchase where the merchant issues an invoice upfront containing the IBAN and payment references, and the customer settles the invoice via a bank transfer. It includes the creation of the invoice, the initiation and execution of the payment, the generation of the eReceipt once the payment is matched to the invoice, and the distribution of the attestation to the customer's wallet. In scope are the data flows between merchant, PSP or payment service provider, the customer's bank and the eReceipt issuer, as well as basic verification of the attestation by relying parties. Out of scope are complex collections workflows (reminders, dunning strategies), detailed risk and credit assessments, and non-IBAN payment methods.

This scenario is important because IBAN-based payments with upfront invoices are widespread in B2B and in many high-value B2C purchases (utilities, subscriptions, professional services, equipment), where proof of payment and reconciliation are critical. It demonstrates how standardized eReceipts can reduce manual reconciliation efforts and disputes for merchants, while enabling banks to enrich their account-based services (invoicing, expenses, cash-flow insights) with a reliable and structured view of the underlying transaction. It also proves that the eReceipt model is not limited to card rails but can support account-to-account payment schemes, which is key for future convergence with SEPA, instant payments and upcoming PSD3/EUDI use cases.

The scenario is based on the following documentation:

- WeBuild Architecture & Integration Blueprint Reference Document
[WE BUILD — Architecture & Integration Blueprint \(D4.1\)](#)
- PA4 stock taking document
<https://portal.webuildconsortium.eu/group/pa4-business-payments/files?mid=5857&fid%5B0%5D=236&fid%5B1%5D=237&fid%5B2%5D=4212>
- PA2 stock taking document
<https://portal.webuildconsortium.eu/group/pa2-consumer-payments/files?mid=5920&fid%5B0%5D=201&fid%5B1%5D=202&fid%5B2%5D=4208>
- European Business Wallet Regulation (draft)
[EUR-Lex - 52025PC0838 - EN - EUR-Lex](#)
- EUDI Wallet Architecture and Reference Framework (ARF) – version 2.9
[European Digital Identity](#)
- Domain-specific standards for eInvoicing and payment interoperability (Peppol BIS Billing 3.0, ISO 20022, EN 16931, HEROJson)

2 Scenario specification

2.1 Introduction

This scenario 1.2 (PA4) covers B2B payment with IBAN. The objective of this scenario is to demonstrate how the eReceipt is not only generated and verified, but also securely stored in the buyer's business wallet, so that corporate users can retain a standardized, reusable proof of each transaction directly within their existing wallet environment.

Key Characteristics:

- Timeline: Payment completes in seconds (vs. days/months for eInvoices)
- Relationship: Merchant does not know the customer (no KYC/KYB); merchant validation is performed by acquirers, payment facilitators/aggregators, and card rails (domestic or international card schemes)
- Typical B2B Use Case: Expense management scenarios (ferry tickets, parking, etc.)
- ERP systems are used to generate payment order to pay with credit transfer

2.2 Scenario pre-conditions

To ensure the successful execution of this scenario, the following preconditions must be met:

Before the main workflow can start, each actor must already be provisioned with the right credentials and connections. The bullets below list the one-time setup steps that must have happened *before* the eInvoice is sent; they are not part of PA4's runtime flow, but PA4 will not execute correctly without them.

Seller pre-requisites

- The Business Register has issued an EBWOID to the Seller, provisioning the Seller's Business Wallet.
- The Seller is connected to an Invoice Processor (its own internal system or equivalent e-invoicing infrastructure) through which the eInvoice can be sent.

Category	Wallet	Attestation	Details
Identity Setup	EUDI Wallet	Personal Identification Data (PID)	Individual identity attestation stored in EUDI Wallet
Business & Banking Setup	EU Business Wallet	EU Business Wallet Organizational ID (EUBWOID)	Business registration attestation stored in EU Business Wallet
	EU Business Wallet	EU Company Certificate (EUCC)	Verified legal entity attestation
	EU Business Wallet	IBAN Attestation	Issued following bank account onboarding via PA3 Scenario 1 and/or 3
Operational Readiness	EU Business Wallet	Invoicing Capability	Ability to issue structured invoices (Peppol BIS Billing 3.0, EN 16931)
	E-commerce platform		
	External system	Bank integration	
	External System	Invoice Network Integration	Peppol Access Point or equivalent e-invoicing infrastructure

Buyer pre-requisites

- The Authorised Person's EUDI Wallet is in the "Active" state (see §2.2 for what this entails and why it is out of scope for PA4).
- The Business Register has issued an EBWOID to the Buyer, provisioning the Buyer's Business Wallet.
- A Bank Wallet has been defined for the Buyer at its Home Bank.
- The Buyer is connected to an Invoice Processor (its own internal system or equivalent e-invoicing infrastructure) so that incoming eInvoices land in the Business Wallet.
- The Buyer is connected to a Payment Processor (its own internal system or an external PSP) so that card payments can be initiated.

Category	Wallet	Attestation	Details
Identity Setup	EUDI Wallet	Personal Identification Data (PID)	Individual identity attestation stored in EUDI Wallet
Business & Banking Setup	EU Business Wallet	EU Business Wallet Organizational ID (EUBWOID)	Organizational identity attestation stored in EU Business Wallet
	EU Business Wallet	EU Company Certificate (EUCC)	Verified legal entity attestation
	EU Business Wallet	IBAN Attestation	Issued following bank account onboarding via PA3 Scenario 1
	EBW	EBW linkage with bank for PoA	
	EBW	Capability to receive and handle eReceipt	
Supplier Relationship	EU Business Wallet	Supplier Onboarding (KYS)	Completed via BU1 Know Your Supplier process – establishes trusted supplier relationship and validates seller credentials Relevant for Scenario 1.1

2.3 Scenario main flow

The flow is broken into six steps that always run in the same order:

- (1) pick the legal entity
- (2) receive an invoice
- (3) initiate the IBAN payment transfer
- (3) token validity check
- (4) authorise the legal entity (SR/PoA)
- (5) settle
- (6) issue the eReceipt.

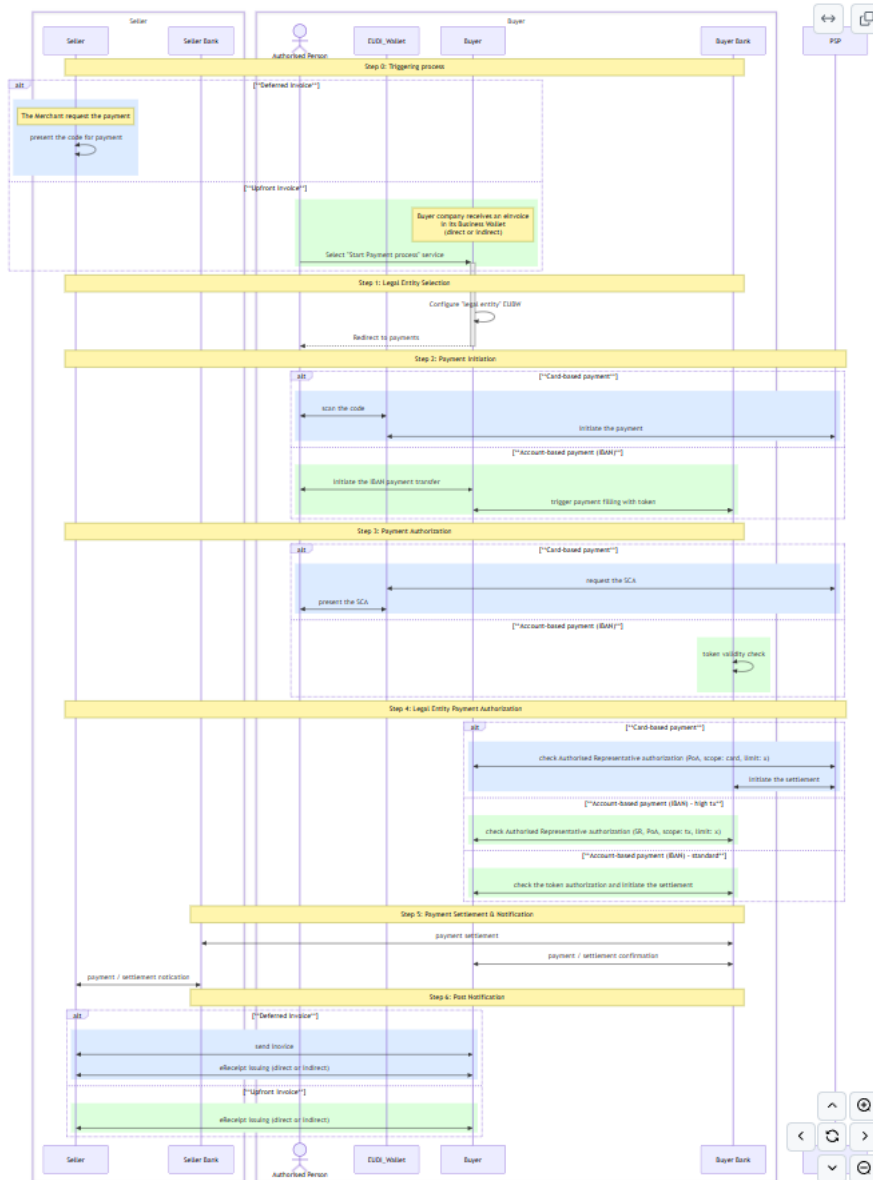
Illustrations are presented in annexe.

The sequence diagrams are stored in Github

[wp3-technology-standards/sequence-diagrams/PA4](https://github.com/wp3-technology-standards/sequence-diagrams/PA4) at main · [webuild-consortium/wp3-technology-standards](https://github.com/wp3-technology-standards)

Note: Color legend:

- Blue – Deferred Invoice
- Green – Upfront Invoice
- White – Applicable to both scenarios



2.4 Challenges and barriers

As outlined in the specification document, this use case is based on a set of assumptions that allow coverage of the majority of relevant scenarios. However, special or edge cases would need to be revisited and addressed when designing a production-grade implementation.

Key challenges that this use case highlights include the need for clear decisions and technical specifications regarding:

- Wallet discovery mechanisms
- Mutual authentication between participating parties
- Automation capabilities related to the European Business Wallet (EBW)
- The trust infrastructure, particularly for (Q)EAAs and certificates
- The core verification process, including which checks will be performed within the WE BUILD framework to ensure that attestations are authentic, valid, and trustworthy

2.5 Working Assumptions

The MVP cannot exercise the full target architecture, so we pin several variables to known values. Each subsection below states what we assume to be true for one perspective (Seller, Buyer, Authorised Representative, and the two wallets), so reviewers can quickly find the assumptions that affect their area. If any of these assumptions fails in practice, the corresponding step in §8 will not behave as described.

2.5.1 Seller (Holder)

- Holds an active EBW with only the minimum set of attestations required to execute PA4.
- Not required to complete Home-Bank onboarding (PA3) or KYS onboarding (BU1 – KYS).
- Classified exclusively as low- or medium-risk.

2.5.2 Buyer (Relying Party)

- Holds an active EBW with only the minimum set of attestations required to execute PA4.
- Not required to complete Home-Bank onboarding (PA3) or KYC onboarding (BU1 – KYC).
- Onboarding of the Authorised is performed as part of end-customer onboarding (not as a separate business-representative onboarding under PA2).
- Business Wallet is assumed to contain valid Signatory Rights (SR) attestations together with the corresponding PoA for the Authorised Representative.
- For IBAN-based transactions, the IBAN information provided in the eInvoice is assumed trusted (IBAN validation is out of scope, see §2.2). IBAN validation is via the trusted bank issuer.

2.5.3 Authorised Person

- Holds a valid EUDI Wallet containing a PID credential.
- Holds the SCA attestation in the wallet.
- Validation of the company's list of Authorised Persons (SR) is out of scope for the MVP.
- Performs SCA using possession of the wallet device combined with PIN or biometric authentication.

2.5.4 Holder Business Wallet

- Automatic flow
- Mutual authentication is enabled by default; no TLOL or device-binding checks are applied.
- The buyer wallet is pre-authorised to both present and receive attestations; no additional configuration is supported in the MVP.
- The Business Wallet accepts credential offers automatically when an active corporate authorisation session is already established.
- Manual flow
- Mutual authentication is reduced to a visual verification step.
- Authorization is reduced to a visual check and manual approval.

2.5.5 Relying-Party Business Wallet

- Attestation verification for each attestation is limited to:
- Cryptographic validation (Section 4.2.1).
- Issuer identification against an internal trusted list (Sections 4.2.2 – 4.3.3).

2.5.6 General

- The payment process is executed sequentially in a single-user flow.
- The eInvoice is assumed to have already been received in the Business Wallet.
- The process concludes with the issuance of the eReceipt attestation into the Business Wallet.
- No attestation is issued to the Authorised Person's EUDI Wallet.

3 Detailed scenario flow

The diagram below is the single picture to remember. Read it top-to-bottom: the eInvoice arrives, the Authorised Person starts the process at the Bank, and each subsequent block (Steps 1–6) lines up with one of the detail subsections that follow. alt ... else ... end blocks represent the card-vs-IBAN branches.

3.1 Step 1: Legal Entity Selection

The Authorised Person may represent more than one company, so the first thing the Bank needs to know is on whose behalf this payment is happening. Nothing in the rest of the flow makes sense until this binding is made.

Goal: Identify which legal entity the Authorised Person is acting on behalf of and start the payment process.

Pre-condition: eInvoice present in Buyer's EBW; Authorised Person authenticated to the Bank channel.

Actors: Authorised Person, Bank.

Post-condition: Bank session bound to the selected legal entity.

Errors / fallbacks: Legal-entity discovery fails → Authorised Person is prompted to re-select; session is not bound.

3.2 Step 2: Payment Initiation

Here the workflow forks for the first time, depending on the payment rail chosen by the Authorised Person. The card path involves the EUDI Wallet and the PSP; the IBAN path stays inside Buyer ↔ Bank. After this step the rails do not re-merge until settlement.

Goal: Initiate payment over the chosen rail.

Branches:

IBAN: Authorised Person triggers IBAN transfer from Buyer → Bank receives payment filling with a token.

Post-condition: A pending payment instruction exists at PSP or Bank.

Errors / fallbacks: Code scan fails (card) or token generation fails (IBAN) → process aborts before authorization.

3.3 Step 3: Payment Authorization

This step answers the question "is the right person approving this payment?". For card payments, that means a full SCA prompt against the EUDI Wallet; for standard IBAN payments, the Bank's pre-issued token is treated as a proxy for that approval, so no SCA is shown to the user.

Goal: Authenticate the Authorised Person for the payment.

Branches:

IBAN standard: Bank performs an internal token validity check (no SCA prompt).

Post-condition: Payment is authorised at the rail-specific level.

Errors / fallbacks: SCA failure → payment is rejected; token invalid → IBAN flow aborts.

3.4 Step 4: Legal Entity Payment Authorization

Step 3 proved who is approving; Step 4 proves they are allowed to approve on behalf of the company, for this rail and this amount. This is where Signatory Rights and Power of Attorney attestations are checked. A high-value IBAN transaction triggers the strictest check (SR + PoA with a transaction-level limit).

Goal: Confirm the Authorised Person has authority for the legal entity to execute this payment.

Branches:

IBAN – high tx: Bank verifies Authorised Person authorization against Buyer (SR + PoA, scope: tx, limit: x).

IBAN – standard: Bank verifies token authorization against Buyer and initiates settlement.

Post-condition: Settlement is authorised.

Errors / fallbacks: Missing or insufficient SR/PoA → settlement is not initiated.

3.5 Step 5: Payment Settlement

With both the person and the company authorised, the Bank performs the actual movement of funds. From the user's perspective this step is largely invisible; they will only see the resulting confirmation.

Goal: Move funds and notify Buyer.

Flow: Bank performs settlement internally and confirms to Buyer.

Post-condition: Payment is settled and Buyer holds a settlement confirmation.

3.6 Step 6: eReceipt Issuance

The eReceipt is the persistent, verifiable proof that the invoice was paid, and its delivery to the Buyer's EBW is the formal end of the workflow. Note that the receipt is a company-level artefact: it lands in the Business Wallet, not in the Authorised Person's EUDI Wallet.

Goal: Deliver an eReceipt attestation to the Buyer's EBW.

Flow: Buyer obtains the eReceipt from Seller (direct or indirect).

Post-condition: eReceipt attestation is stored in Buyer's EBW. No attestation is issued to the Authorised Person's EUDI Wallet.

4 Roles and participants

4.1 Scenario roles and participants

Primary role	UC partner Name	Country
Buyer (Relying party for eReceipt)	SME (to identify)	Germany or Switzerland
Seller (Authentic source for eReceipt)	Bosch	Germany
Wallet provider (for buyer)	SIROS * (EBW)	Germany
Wallet provider (for seller)	Procivis (EBW)	Switzerland
Intermediary for ERP Buyer system	DATEV	Germany
Intermediary for eReceipt	Bosch (ERP system)	Germany
IBAN Attestation	Deutsche Bank	Germany

Authentic sources in this use case are needed for companies and financial institutions. The later require for the MVP flow an EBWOID and EUCC, therefore less data requirements arise for authentic sources covering this.

4.2 Additional roles and partners

Current working assumption is that we achieve conformance within the use case. And that any wallet provided within the country can be used across borders. So no specific matching of countries is done here.

4.3 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.

Overview over the attestations and required attribute are here

[webuild-attestation-rulebooks-catalog/rulebooks at main · webuild-consortium/webuild-attestation-rulebooks-catalog](#)

5.2 Attestations to be provided by Authentic sources, other than the company

...

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	Requirements
PID	Personal Identification Data	PA1 / Member state PID Provider	eIDAS 2.0 Level of Assurance High
EUBWID	EU Business Wallet Organisational ID	PA1 / EBW Provider	Issued upon EBW activation; links natural person to legal entity
EUCC	EU Company Certificate	PA1 / National business register	Authentic source: national commercial register (PRH, Handelsregister, Bolagsverket)
IBAN Attestation	Bank account ownership confirmation	PA3 Scenario 1 and/or 3	Issued by account-holding bank following onboarding. Required for SEPA payment path (Scenario 1.1).
SCA Attestation	Strong Customer Authentication proof	PA2 B1 / PA3 / Issuing bank	PSD2/PSR compliant SCA. Card path: EMV chip+PIN or EUDI Wallet SCA. IBAN path: bank SCA.
KYS (Supplier Onboarding)	Know Your Supplier — trusted supplier relationship	BU1 / Buyer EBW	Completed via BU1 KYS process. Scenario 1.1 only (not required for 1.2 expense management).

5.3 Created attestations in the scenario by the companys' EBW

EAA – Attestation issued by the company out of the Business Wallet

Attestation name	Short description	Issuer	For Countries	Applicable domain standards
DS-011 eReceipt (vReceipt)	Structured proof of purchase — items, VAT, merchant identity, payment verification	Merchant or PSP/Acquirer, via eReceipt Intermediary (technical issuer)	FI, DE, SE	SD-JWT VC (EWC RFC011), HeroJSON field names, CEN/TS 16931-8:2024, OIDC4VCI (RFC001), OIDC4VP (RFC002)
DS-012 Payment Attestation	Bank-issued payment event confirmation — amount, parties, rail-specific verification data	Issuing Bank (card) / Account-holding Bank (SEPA)	FI, DE	SD-JWT VC, ISO 20022 (pain.001, camt.054), EMV Specifications, EPC125-05 SCT Rulebook
DS-013 eReceipt Routing Credential	Employer-issued routing credential — maps card/IBAN tokens to Business Wallet endpoint (early draft)	Employer (via EBW or HR system)	FI, DE, SE	SD-JWT VC, OIDC4VCI (RFC001), OIDC4VP (RFC002), ARF 1.6
IPC (Invoice Payment Confirmation)	Payment confirmation for structured e-invoice — links Peppol invoice to SEPA payment	Account-holding Bank	FI, DE	SD-JWT VC, Peppol BIS Billing 3.0, EN 16931-1, ISO 20022

Annex 1 – Requirements for scenario roles

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

- **High-Level Requirements:**

For banks, the impact is concentrated in digital channels and verification logic, not in core banking. They will need to adapt their mobile/web channels to display an additional “digital receipt” element on card transactions in the pilot perimeter, and implement lightweight verification and matching to their internal transaction records. Operational units (customer service, disputes, compliance) should be informed and involved in evaluating how eReceipts change the handling of claims and controls, without changing formal regulatory processes during the pilot.

- **What Participants Need to Do (“Shopping bag”):**

At a non-technical level, participants are expected to:

- Ensure that invoices and related payment instructions contain the data required to construct a compliant eReceipt (amounts, VAT, merchant identity, references, due date, line items where relevant).
- Implement the ability to generate an eReceipt once the IBAN payment has been successfully executed and reconciled with the invoice, applying the rulebook’s data and integrity rules.
- Deliver the eReceipt to the holder through at least one standard distribution channel (EBW, banking app, portal) and maintain a reference enabling subsequent verification.
- Act as relying parties capable of verifying the attestation’s integrity, trust properties

(issuer, status, validity) and basic consistency with their own records when an eReceipt is presented.

For banks and other relying parties, expectations are explicitly:

- To consume eReceipts for IBAN-based payments in at least one digital channel (typically online or mobile banking) and link them to the corresponding account transactions and/or invoice records.
- To implement a basic verification path: confirming that the eReceipt is syntactically valid, originates from a trusted issuer, and is coherent with known payment and invoice data (amount, counterpart, reference, date).
- To provide a clear, business-oriented view of the eReceipt to end-customers (or corporate users), focused on reconciliation, proof of payment and accounting/fiscal use, rather than on technical details.
- To participate in structured feedback on customer experience, operational impact (reconciliation, disputes, customer service) and compliance benefits,

The key message to banks is: you are not asked to change your SEPA engines or core accounting; you are asked to plug a standardized “proof of invoice payment” on top of existing account transactions and invoice management, and to make it visible and verifiable in your channels.

Annex 2 - EN 16931-1:2026 Revision Analysis

This section provides a strategic analysis of the EN 16931 standard revision and its implications for the PA4 eReceipt and eInvoice attestations.

E.1 Standard Versioning

Current status: **CEN approved the revised EN 16931-1 on 13 February 2026** (formally published as EN 16931-1:2026). Definitive Text available since 18 March 2026. National Standard Bodies must publish by 31 May 2026.

Previous version: EN 16931-1:2017 was the original B2G e-invoicing standard mandated by Directive 2014/55/EU. The 2026 revision is **not backward compatible** — invoices valid under 2017 will not pass 2026 validation.

E.2 Key Changes in the 2026 Revision

ViDA-Driven Requirements

- IBAN fields: expanded payment information to support Digital Reporting Requirements (DRR) from 1 July 2030
- Margin scheme support: national VAT special schemes now standardised
- Goods/services indicator: new field distinguishing product types for CTC reporting
- Triangulation indicators: support for VAT simplification in three-party chains

B2B Extensions

- Multiple order references per invoice: single invoice can reference several purchase orders
- Multiple buyer identifiers: supports the payer ≠ buyer dynamic central to PA4 Scenario 1.2
- XML attachments: structured data can be embedded within the invoice
- Advanced payment terms: early payment discounts, late-payment charges
- New VAT codes and exemption reason codification

Invoice Management

- Issuance timestamp: standardised field for exact invoice creation time (relevant for real-time reporting)
- Corrective invoice sequencing: formalised handling of credit notes and corrections

E.3 Syntax Binding Status

Binding	Status (April 2026)	Implication
UBL 2.5	TS draft accepted internally by TC 434. Formal vote scheduled July 2026.	Peppol BIS 4.0 will be built on this. Cannot build conformant implementations until finalised.
UN/CEFACT CII D25A	TS draft accepted. Same July 2026 vote timeline.	XRechnung 4.0 (Germany) will align. Critical for DE pilot partners.
Peppol BIS 4.0	Under development by OpenPeppol. Merges BIS 3.0 + PINT into unified standard.	PA4 Scenario 1.1 eInvoice path depends on this. Timeline not yet confirmed.

E.4 CEN/TS 16931-8:2024 — The eReceipt Standard

CEN/TS 16931-8:2024 (published October 2024) defines the *semantic data model for e-receipts and simplified electronic invoices*. This is the CEN-level standard that directly corresponds to DS-011 eReceipt content.

The standard establishes a semantic model including essential information elements for legal (including fiscal) compliance and cross-border interoperability. It covers both B2B expense management and B2C consumer receipts. The 110-page specification provides the formal basis for the HeroJSON field names used in DS-011.

Key alignment: DS-011 v2.2 attributes map directly to CEN/TS 16931-8 business terms. The VAT codes in DS-011 (vats[].VATCode) use the EN 16931-1 category codes (S, Z, E, etc.). This alignment ensures that eReceipts are interoperable with eInvoice infrastructure.

E.5 Migration and Backward Compatibility

The 2026 revision is explicitly **not backward compatible** with EN 16931-1:2017. This has significant implications:

- ERP systems, access points, and matching workflows will all need updates
- Peppol BIS 4.0 will be the unified standard — current BIS 3.0 implementations must migrate
- Denmark has announced Nemhandel BIS 4 with a 2029 migration timeline, cancelling OIOUBL 3.0
- Germany's XRechnung 4.0 will align with EN 16931-1:2026 — critical for DATEV/Bosch pilot path

For PA4 pilot: The pilot should be designed to work with both EN 16931-1:2017 (current production) and EN 16931-1:2026 (target). DS-011 and IPC attestation schemas should support both versions during the transition period (estimated through ViDA 2030 go-live).

E.6 Change Pressures Not Yet Addressed — Future Roadmap

The following change pressures are visible but not yet incorporated into EN 16931 or the PA4 specification. They represent potential future roadmap items.

Pressure	Description	PA4 Relevance
PSD2/PSR vs. eIDAS2 SCA gap	PSD2 SCA requires dynamic linking; eIDAS2 Strong User Authentication (SUA) does not. PSPs unsure which to implement. PSR (replacing PSD2) expected formal adoption mid-2026, effective 2028.	Directly affects PA4 Block 3 (SCA). MVP uses EMV chip+PIN (bypasses the conflict). EUDI Wallet SCA path blocked until PSR clarifies.
CSRD Scope 3 emissions data	Corporate Sustainability Reporting Directive requires Scope 3 (supply chain) emissions data from 2026. Structured receipts could carry CO2 data per product line.	DS-011 already includes journey{} object for travel emissions. Future extension: products[].carbonFootprint field. Not in MVP but architecturally prepared.
Real-time DRR reporting	ViDA Pillar 1 mandates real-time Digital Reporting Requirements from 1 July 2030. Requires invoice data transmission to tax authorities within 5 days of issuance.	eReceipts with itemised VAT (DS-011) are DRR-ready. Could serve as automated tax reporting input. Future extension beyond expense management.
Agentic commerce / AI-initiated payments	PA2 Risk & Fraud WG (Q4) identifies AI-initiated payments as emerging fraud/liability concern. No regulatory framework yet.	Future PA4 use case: AI-driven expense submission and approval. ReceiptHero's structured data enables automated policy checks. Liability model undefined.

Payment Wallets WG	New PA2 working group (PayPal leading, kickoff June 2026) analysing EUDI Wallet impact on existing payment wallets (Apple Pay, Google Pay, PayPal).	eReceipt delivery channel. If payment wallets become EUDI Wallet intermediaries, the receipt delivery question becomes: which wallet receives the receipt? DS-013 routing solves this. ApplePay & GooglePay supported in production.
EN 16931 Part 8 → full EN promotion	CEN/TS 16931-8 is currently a Technical Specification (TS), not a full European Norm (EN). If e-receipts become mandated (like e-invoicing via Directive 2014/55/EU), promotion to EN may follow.	Would create a legal mandate for structured receipts, analogous to B2G e-invoicing. Strongest possible regulatory tailwind for PA4 eReceipt adoption.
Cross-border VAT refund automation	Current VAT refund for cross-border business purchases (Directive 2008/9/EC) requires manual documentation. Structured eReceipts could automate the claim.	DS-011 contains all required data: merchant VAT ID, itemised VAT amounts per rate, payment proof. Future integration with Member State refund portals.

ANNEXE 3 _ illustration of the workflow to issue an eReceipt

Figure 1 Pre-condition: KYC/KYS process

Figure 2 Common: card or invoice

Figure 3 Scenario 1.1. SCA of payment

Figure 4 Scenario 1.1. Issuance of eReceipt of card payment

Figure 5 Scenario 1.2. approval of invoice

Figure 6 Scenario 1.2. Payment reception verification delivered to buyer



Payment options sent to your EUDI Wallet

Choose how you want to pay



Secure
End-to-end encrypted
data transfer



Trusted
Based on EU standards
and eIDAS 2.0



Convenient
Fast, simple and
under your control

Card payment approved in your European Digital Identity (EUDI) Wallet

A secure and convenient way to pay online

1. Choose card payment at checkout

2. Select your card in EUDI-wallet

3. Authenticate with fingerprint or PIN code

4. Payment approved securely



Secure
Strong authentication
keeps your payments safe



Privacy first
Your data is protected
and under your control



Convenient
Fast and easy payments
wherever you shop



European solution
Built on EU standards
for trust and interoperability

Receipts in your EUDI Wallet and accounting software

The same receipt – securely stored and automatically available in your accounting

The diagram illustrates the secure sharing and syncing of a receipt between an EUDI Wallet and Accounting software. A smartphone on the left displays the EUDI Wallet interface, showing a receipt from Nordic Store for Wireless Headphones. A laptop on the right displays the Accounting software interface, showing the same receipt. A cloud icon with a checkmark and arrows indicates the secure sharing and syncing process.

EUDI Wallet

Accounting software

Securely shared and synced

The receipt is securely delivered via the Peppol Network and automatically available in your accounting system.

- Reliable**
Data delivered via Peppol Network
- Secure**
End-to-end encrypted and compliant
- Efficient**
No manual entry – saves time and reduces errors

Peppol e-invoice – Verified and ready for approval

Secure, compliant and fully traceable

The diagram illustrates the verification and approval process for a Peppol e-invoice. It shows the invoice details, the automatic verification process, and the final approval step.

INVOICE

Invoice number: INV-2024-0515
Issue date: 15 May 2024
Due date: 29 May 2024

Seller: Nordic Solutions Oy
Business ID (VAT): FI12345678
Address: Mannerheimintie 12 B, 00100 Helsinki, Finland

Buyer: Acme Corporation Oy
Business ID (VAT): FI87654321
Address: Porkkalankatu 1, 00180 Helsinki, Finland

Item: Wireless Headphones, 10 pcs, Unit price: 129,00, VAT: 24%, Amount: 1 290,00

Subtotal: 1 290,00
VAT 24%: 309,60
Total EUR: 1 599,60

Payment details: IBAN: FI12 3456 7890 1234 56, BIC: NDEAFIHH, Bank: Nordea Bank Abp

Other information: Peppol format: UBL 2.1, Peppol ID (Seller): 0192:FI12345678, Peppol ID (Buyer): 0192:FI87654321, Profile ID: urn:fcp:peppol.eu:2017:poacc:billing:01:1.0, Customization ID: b3f2a6d9-7c1e-4b09-8e3e-0b5f9e8c1d2a, Transmission ID: b3f2a6d9-7c1e-4b09-8e3e-0b5f9e8c1d2a

Automatic verification:

- IBAN verified: Nordea Bank Abp
- VAT number verified: FI12345678
- Peppol format valid: UBL 2.1
- Invoice integrity: No changes detected
- Seller identity verified: Nordic Solutions Oy

All checks passed. Ready for approval.

Business Wallet Invoice approval

From: Nordic Solutions Oy
Invoice number: INV-2024-0515
Amount: 1 599,60 EUR
Due date: 29 May 2024

IBAN: FI12 3456 7890 1234 56
VAT number (Seller): FI12345678
Peppol validation: All checks passed

This invoice is valid. You can approve it for payment.

Approve invoice
Reject invoice

Secure: End-to-end encrypted data exchange
Compliant: Based on EU standards and eIDAS 2.0
Efficient: Faster processing, fewer errors
Sustainable: Paperless and better for the environment

Invoice paid – Reception verified

The invoice is paid and successfully received by the buyer

✓ PAID

✓ Reception verified



INVOICE

Invoice number INV-2024-0515
Issue date 15 May 2024
Due date 29 May 2024



Peppol ID (Seller)
0192:FI12345678
Peppol ID (Buyer)
0192:FI87654321

Seller

Nordic Solutions Oy
Business ID (VAT)
FI12345678 ✓
Address
Mannerheimintie 12 B
00100 Helsinki, Finland

Buyer

Acme Corporation Oy
Business ID (VAT)
FI87654321 ✓
Address
Porkkalankatu 1
00180 Helsinki, Finland

Description	Quantity	Unit price	VAT %	Amount
Consulting services	10	120,00	24%	1 200,00
Software license	1	800,00	24%	800,00
			Subtotal	2 000,00
			VAT 24%	480,00
			Total EUR	2 480,00

Payment details

IBAN FI12 3456 7890 1234 56 ✓
BIC NDEAFIHH
Bank Nordea Bank Abp

Additional information

Invoice format UBL 2.1
Customization ID urn:fdc:peppol.eu:2017:poacc:billing:01:1.0
Profile ID urn:fdc:peppol.eu:2017:poacc:bis-invoice:3.0
Transmission ID b3f2a6d9-7c1e-4b09-8e3e-0b5f9e8c1d2a



This invoice was received via the Peppol Network.
This invoice has been paid and the reception has been verified by the buyer.

Status

- ✓ **Paid**
Payment completed on 29 May 2024
- ✓ **Reception verified**
Verified by the buyer on 29 May 2024

What this means

- ✓ **Delivered**
Invoice successfully delivered via the Peppol Network
- ✓ **Paid**
Payment has been received
- ✓ **Reception verified**
Buyer has confirmed receipt of the invoice

Benefits

- ✓ **Secure & compliant**
Meets EU standards and regulations
- ✓ **Efficient**
No manual handling, real-time status
- ✓ **Sustainable**
Paperless process