s

OOTS and EUDI Wallet Synergies

Findings and Observations from a Proof of Concept

Keilalahdentie 2-4
P.O.Box 2
FI-02101 Espoo
Finland

Table of Contents

List of Figures and Tables

Figures

Tables

1 Executive Summary

This report presents the findings of the OOTS Wallet Proof of Concept, carried out in the context of the Nordic-Baltic OOTS 2.0 cooperation. The PoC examined practical synergies between the Once-Only Technical System and the European Digital Identity Wallet, focusing on how OOTS-related evidence capabilities could support wallet-based use of public-sector information. In this way it also contributes to the project's objective of demonstrating the benefits of structured data exchange and reuse within the Once-Only Technical System (OOTS), from the perspectives of both competent authorities and end users.

The main finding is that OOTS and the EUDI Wallet can support each other through both user experience and investment synergies. OOTS-related service flows can be extended with wallet issuance and later wallet-based presentation, while OOTS-related investments in source-system integrations, evidence definitions, data models and semantic work can provide a reusable foundation for issuing wallet-compatible public-sector credentials.

The PoC demonstrated these synergies through two use cases. The first use case added a wallet option to an existing OOTS-based evidence flow at the Preview Space, where proof-of-residence evidence was retrieved from an authoritative source, prepared for wallet issuance and issued to a test mobile wallet as a wallet-compatible attestation. The same attestation could later be presented from the wallet back into an OOTS-related service process. The second use case examined the National Digital Credential Service as a broader national model in which users can request supported public-sector attestations through a shared national service path and receive them in their EUDI Wallet. In this model, OOTS-related integrations, evidence definitions and data models can be reused, while a dedicated issuing capability handles the wallet-facing issuance interaction.

The practical value of the synergy is that public administrations can build on existing OOTS-related work instead of starting each EUDI Wallet credential implementation from an individual register. Where OOTS-related integrations, evidence definitions, semantic assets and data models already exist, they can reduce duplicate work and lower the threshold for making selected public-sector attestations available to the wallet. This is relevant for EUDI Wallet adoption because broad everyday use depends on credentials that users can present and that public authorities and businesses can rely on in real service processes, including credentials based on residence, education or other public-sector information.

OOTS and the EUDI Wallet serve complementary roles. OOTS supports cross-border evidence retrieval and exchange between authorities for administrative procedures, while the EUDI Wallet supports user-controlled holding and later presentation of wallet-compatible attestations based on trusted public-sector information.

The PoC demonstrated feasibility at proof-of-concept level in a test environment. Production use would still require decisions on the legal basis, issuer role, trust framework, responsibility allocation, lifecycle and revocation handling, funding, ownership and long-term operation. For Finland, existing OOTS capabilities provide a practical starting point for further assessment. KEHA’s current role in national OOTS implementation makes it a possible operator for a shared National Digital Credential Service, provided that the legal issuer role and mandate are clarified separately.

The next step is to assess which public-sector evidence types are most suitable for wallet issuance, where OOTS-related capabilities can be reused, and what legal, organisational and operational arrangements would be required. Nordic-Baltic cooperation could support this work by comparing selected evidence areas, identifying common attributes and testing credential models before wider EU-level alignment is complete.

2 Introduction

2.1 Background

This report documents the KEHA OOTS Wallet Proof of Concept and its findings in the context of the Nordic-Baltic OOTS 2.0 cooperation. The Proof of Concept was carried out as part of broader work to understand how structured evidence exchanged or made available through OOTS-related capabilities could be reused and utilised by competent authorities and end users. Other features of the Proof of Concept will be presented in videos, other planned outputs and in the final report of the OOTS 2.0 project.. This report is intended to provide a clear account of the PoC background, implementation context and observed results for public-sector officials and decision-makers, including the Nordic Council of Ministers, which funded the wider OOTS 2.0 cooperation.

The Once-Only Technical System (OOTS) is part of the implementation of the Single Digital Gateway Regulation. It provides a European framework for exchanging evidence between competent authorities across Member States. Its purpose is to reduce the need for citizens and businesses to provide the same information repeatedly when completing administrative procedures in another Member State. Instead, with the user's request and consent, the necessary evidence can be retrieved from the relevant authoritative source and transmitted through the OOTS infrastructure to the competent authority that needs it.

The European Digital Identity Wallet is another major European digital public service initiative. Under the revised eIDAS Regulation, EU Member States are required to provide at least one European Digital Identity Wallet to their citizens, residents and businesses. The wallet is intended to enable users to identify themselves, store and manage digital credentials, and present information in a user-controlled way across public and private digital services. This makes the EUDI Wallet directly relevant to the future use of digital evidence: while OOTS supports the retrieval and exchange of evidence from authoritative sources, the wallet provides a channel through which evidence-derived electronic attestations or credentials can be held, presented and reused by the user.

OOTS and the EUDI Wallet address partly different but closely related needs. OOTS is primarily designed for the trusted exchange of evidence between public authorities in the context of administrative procedures. The EUDI Wallet, in turn, enables evidence-derived electronic attestations or credentials to be placed under the user's control and presented by the user in later service interactions. This creates a natural area of complementarity: evidence retrieved from authoritative sources through OOTS-related capabilities may, where legally and technically appropriate, also be transformed into wallet-compatible digital credentials that can be reused by the holder. The European Commission's OOTS–EUDI Wallet synergy work has identified this relationship as an important area for further development, including potential benefits such as reduced administrative burden, improved user experience and more efficient reuse of public-sector digital infrastructure.

The KEHA OOTS Wallet PoC was carried out in this broader European and Nordic-Baltic context. The PoC formed part of the Nordic-Baltic OOTS 2.0 project, a cooperation project between the national SDG coordination teams of the Nordic and Baltic countries, led by Finland and funded by the Nordic Council of Ministers' Cross Border Digital Services Programme under the Nordic Council of Ministers for Digitalisation. The PoC was therefore a practical contribution to the wider question of how OOTS-based evidence exchange and EUDI Wallet capabilities could support each other in future European digital public services and how the Nordic and Baltic countries can benefit from the synergies created through the interoperability of these two systems.

Finland has already implemented a practical national OOTS foundation. KEHA Centre acts as the national coordinator for the Single Digital Gateway implementation in Finland and has implemented centralised national OOTS services, including data retrieval and preview services for citizens and businesses, as well as data transmission and data management services for authorities. Finnish OOTS services already cover evidence from national authoritative sources such as the Population Information System and the Trade Register, and the scope is expanding to further data sources such as education records. This creates a concrete basis for exploring how OOTS-related evidence capabilities could also support the issuance of wallet-compatible electronic attestations or credentials.

The broader significance of this lies in the potential reuse of public-sector evidence capabilities. OOTS already requires evidence types, authoritative sources, data models and integration paths to be identified for administrative procedures. If this same groundwork also supports wallet-compatible electronic attestations or credentials, Member States could use existing OOTS-related capabilities as a starting point for EUDI Wallet implementation across selected evidence types. This could make EUDI Wallets more useful for citizens and businesses by increasing the range of authoritative public-sector information that can be held and presented through the wallet. A broader supply of useful attestations would give users more reasons to adopt the wallet, support the reuse of evidence across service interactions, reduce repeated evidence requests and manual checks in service processes, improve the return on public-sector investments in OOTS capabilities, and make the wallet ecosystem more credible and attractive for public and private service providers.

Against this background, the PoC explored how OOTS-related evidence capabilities could be combined with wallet issuance and presentation patterns. This question is increasingly relevant because OOTS is becoming an operational infrastructure for the exchange of evidence between authorities, while EUDI Wallets are expected to provide a user-controlled channel for holding and presenting wallet-compatible electronic attestations or credentials. The PoC was designed to examine the practical intersection of these two developments and to provide input for further Nordic-Baltic and European discussion on how their synergies could be realised.

2.2 Purpose of the PoC

The purpose of the PoC was to examine, in practical terms, how OOTS-related evidence capabilities could be combined with EUDI Wallet issuance and presentation patterns. The PoC focused on the question of whether evidence retrieved from authoritative public-sector sources through OOTS-related capabilities could also be transformed into wallet-compatible electronic attestations or credentials that the user can hold, present and reuse in later service interactions.

The PoC was carried out because OOTS and the EUDI Wallet address complementary parts of the same broader policy objective: making public-sector data easier, safer and more efficient to use in cross-border and national digital services. OOTS supports the retrieval and exchange of evidence between competent authorities, while the EUDI Wallet provides a user-controlled channel for holding and presenting digital attestations and credentials. The European OOTS–EUDI Wallet synergy work, where also some Nordic and Baltic Countries have been active, has identified this relationship as a relevant area for further development, including the possibility that OOTS capabilities and common services could support the discovery, issuance or reuse of wallet-compatible attestations.

In this context, the PoC was intended to demonstrate two practical aspects of the synergy. First, it explored whether an existing OOTS-based evidence flow could be extended so that evidence retrieved from an authoritative source could also be made available to the user as a wallet-compatible attestation or credential. Second, it examined the National Digital Credential Service concept as a way to reuse OOTS-related integrations, evidence definitions and data models for wallet-compatible public-sector

credentials derived from national authoritative sources. The work highlights the importance of structured data and its reuse as key enablers of efficient, scalable and interoperable cross-border digital services. This is particularly relevant for the Nordic and Baltic countries, whose data-driven public administrations and mature digital infrastructures provide a strong foundation for maximising the value of existing OOTS investments and demonstrating practical synergies between OOTS and the EUDI Wallet ecosystem. In this context, the Nordic and Baltic countries are well positioned to take a leading role in showcasing the benefits of structured data exchange and reuse for both competent authorities and end users. A broader supply of public-sector attestations could make EUDI Wallets more valuable for citizens and businesses, reduce duplicate integration work for public administrations, and increase the value of investments already made in OOTS capabilities.

The PoC was therefore not designed merely as a technical integration exercise. Its purpose was to provide practical evidence for the wider Nordic-Baltic and European discussion on how OOTS and EUDI Wallet capabilities could support each other. This was aligned with the broader Nordic-Baltic OOTS 2.0 development path, which focuses on improving the current OOTS architecture, user experience and structured data exchange between Nordic and Baltic countries through proof-of-concepts. The PoC was intended to contribute to that wider work by testing selected OOTS/EUDI Wallet synergy patterns in practice and by identifying observations that could guide further technical, organisational and policy-level development.

2.3 Scope and Limitations of the PoC

The PoC was a focused demonstration of selected OOTS and EUDI Wallet synergy patterns. Its scope was limited to exploring how OOTS-related evidence capabilities could support the issuance and later presentation of wallet-compatible electronic attestations or credentials. The PoC did not aim to implement a full production service, replace the existing OOTS evidence exchange model, or define a complete national operating model for wallet-based public-sector attestations. Its role was to provide practical evidence on selected integration and reuse patterns that could inform further national, Nordic-Baltic and European development. The Nordic-Baltic OOTS 2.0 project itself uses proof-of-concepts to explore improvements to OOTS architecture, user experience and structured data exchange, which makes this PoC consistent with the project's wider exploratory approach.

The PoC was based on the assumption that evidence retrieved from authoritative public-sector sources can, where legally and technically appropriate, be transformed into wallet-compatible electronic attestations or credentials. In this report, evidence refers to official documents or data used in the OOTS context, while attestations of attributes or credentials refer to the wallet-compatible representations that can be issued to, held in and presented from the user's wallet. This distinction is important because the PoC did not assume that OOTS evidence would simply be stored in the wallet in its original form. Instead, the relevant question was whether evidence-derived information could be mapped, issued and presented in a form suitable for EUDI Wallet use.

The PoC focused on two main use cases. The first use case examined how an existing OOTS-based evidence flow could be extended with wallet capabilities, including the issuance of an evidence-derived attestation or credential to the user's wallet and the later use of wallet-held information in an OOTS-related service process. The second use case examined whether integrations and data models originally developed for OOTS purposes could also provide a reusable basis for a National Digital Credential Service, through which users could obtain wallet-compatible public-sector attestations or credentials derived from national authoritative sources. The PoC therefore addressed both the extension of an existing OOTS-related flow and the potential reuse of OOTS-related groundwork for a broader wallet-oriented credential issuance service.

The PoC did not seek to resolve all legal, governance or trust framework questions related to production deployment. In particular, it did not define which public-sector bodies should act as issuers of electronic attestations of attributes, how issuer authorisation should be governed, or how long-term responsibilities between evidence providers, wallet providers, relying parties and public-sector authorities should be allocated. These questions are part of the wider European and national EUDI Wallet and OOTS governance discussion. The OOTS/EUDI Wallet synergy work has also identified legal and technical questions around the use of OOTS capabilities and Common Services in EUDI Wallet-related contexts, which indicates that these topics require further policy and governance work beyond a single PoC.

The PoC also did not demonstrate full production-level interoperability across all future EUDI Wallet implementations, attestation formats or relying party environments. It was intended to test selected issuance and presentation patterns and to identify observations that could guide further work. Further testing would be needed to assess interoperability across different wallet implementations, additional evidence types, production trust infrastructures, lifecycle and status mechanisms, and different national service contexts. Similarly, the PoC did not demonstrate that all OOTS evidence types can be converted into wallet-compatible attestations or credentials without further evidence-specific modelling, legal assessment and technical configuration.

The PoC provides a feasibility and learning demonstration of selected OOTS and EUDI Wallet synergy patterns. It provides practical insight into how OOTS-related evidence capabilities and EUDI Wallet patterns can support each other, but it does not by itself establish production readiness, final governance arrangements or full European interoperability. The value of the PoC lies in showing which synergy patterns are worth further development and which technical, organisational and policy questions should be addressed in the next stages.

3 OOTS and EUDI Wallet as Complementary Evidence Channels

3.1 The Once-Only Technical System (OOTS)

The Once-Only Technical System (OOTS) is the European technical infrastructure established to support the exchange of evidence between competent authorities in cross-border administrative procedures covered by the Single Digital Gateway framework. Its purpose is to reduce the need for citizens and businesses to repeatedly collect, download and submit official documents or data that already exist in public-sector authoritative sources. Instead, at the explicit request of the user, the required evidence can be retrieved from the relevant competent authority and transmitted to the authority responsible for the procedure.

In the OOTS context, evidence refers to official documents or data that are needed to fulfil procedural requirements in an administrative procedure. Evidence may consist of structured data or human-readable documents, depending on the evidence type, the source system and the requirements of the procedure. Typical evidence may relate, for example, to population registers, education records, business registers or other public-sector authoritative sources.

The OOTS model is based on the principle that evidence should come from an authoritative source and be exchanged through a trusted process, rather than being manually collected and re-uploaded by the user. This supports both administrative efficiency and trust in the origin of the information being exchanged. OOTS therefore plays an important role in enabling public authorities to rely on evidence retrieved from another competent authority, while reducing the administrative burden on citizens and businesses.

OOTS consists of common European components and national components implemented by Member States. The common components support functions such as identifying relevant evidence types and evidence providers, while national components connect Member State services and authoritative sources to the OOTS framework. The Nordic and Baltic countries have largely adopted a centralised or coordinated national approach to OOTS implementation, where competent authorities connect to the Once-Only Technical System through shared national services.

A key feature of OOTS is that the user remains involved in the evidence exchange process. The user initiates the request and can preview the evidence before it is submitted to the requesting authority. This user involvement is important because OOTS supports administrative procedures through an evidence exchange process in which the user has visibility and control over the use of the evidence.

In this report, the term evidence is used for the official documents or data retrieved and exchanged through OOTS-related processes. Wallet-compatible electronic attestations or credentials are discussed separately in the EUDI Wallet context.

3.2 The European Digital Identity Wallet

The European Digital Identity Wallet is a central element of the revised European digital identity framework. Under the revised eIDAS Regulation, EU Member States are required to provide at least one European Digital Identity Wallet to citizens, residents and businesses. The wallet is intended to provide a secure and user-controlled means for digital identification and for the management of digital documents and attestations across public and private digital services. EU sources describe the wallet as a means for users to securely store, manage and validate person identification data and electronic attestations of attributes.

In the EUDI Wallet context, the user is at the centre of the interaction. The wallet enables the user to hold digital information issued by trusted issuers and to present selected information to relying parties when using digital services. This can include person identification data and electronic attestations of attributes that the user can hold, manage and present through the wallet. The wallet supports both digital identification and the controlled management and presentation of verified digital information.

Wallet-based management of digital credentials changes the way public-sector information can be used in service interactions. In such service interactions, a user can present a wallet-compatible credential that is digitally verifiable and linked to a trusted issuer. This can support more user-controlled service journeys, where the user decides when and where to present information from the wallet, subject to the applicable rules and the relying party's ability to request and verify such information.

For the purposes of this report, the terms electronic attestation of attributes and digital credential are used to describe the same practical concept. They refer to a wallet-compatible digital proof of an attribute or set of attributes that can be issued to the user's wallet, held and managed by the user, and presented by the user in digital service interactions. The more precise regulatory term in the EUDI Wallet and eIDAS context is electronic attestation of attributes, while digital credential is used in this report as a more general and technical term for the wallet-held representation of the same type of information. This differs from the OOTS term evidence, which refers to official documents or data retrieved from authoritative sources and exchanged through OOTS-related processes. The relationship between OOTS evidence and wallet-compatible electronic attestations of attributes or digital credentials is addressed in the following section on OOTS and EUDI Wallet synergies.

3.3 Synergies Between OOTS and EUDI Wallet

OOTS and the EUDI Wallet are complementary mechanisms within the European digital public service landscape. OOTS supports the retrieval and exchange of evidence between competent authorities in the context of administrative procedures, while the EUDI Wallet enables users to hold and present person identification data and electronic attestations of attributes, referred to in this report also as digital credentials. The relationship between the two systems is based on complementarity, with OOTS supporting authority-to-authority evidence exchange and the EUDI Wallet supporting user-controlled holding and presentation of credentials.

The European OOTS and EUDI Wallet synergy work distinguishes between two main categories of synergies. The first category consists of user experience synergies, where EUDI Wallet capabilities can be reused in OOTS-related procedures. These include the use of the wallet as an additional means for identification and authentication, the possibility to receive evidence or procedure outputs in a wallet-compatible format, and the ability to combine evidence presented from the wallet with evidence retrieved through OOTS. These synergies focus on improving the interaction of citizens and businesses with administrative procedures.

The second category consists of investment synergies, where EUDI Wallet-related services reuse OOTS building blocks. These include the use of OOTS Common Services to discover authentic sources, identify evidence providers and issuers, and reuse semantic assets such as data models, rulebooks and schemas. In this sense, OOTS provides reusable infrastructure that can support the discovery, verification and issuance of wallet-compatible digital credentials.

The complementarity between OOTS and the EUDI Wallet can therefore be understood through two directions of reuse. In one direction, OOTS-related procedures benefit from the EUDI Wallet as a user-controlled channel for identification, receiving digital credentials and presenting wallet-held information. In the other direction, EUDI Wallet credential issuance can benefit from OOTS-related work on evidence types, authentic sources and semantic definitions. This work helps define what information can be issued to the wallet, where the information comes from and how it should be interpreted. These two directions reflect the different but connected roles of the systems: OOTS supports trusted evidence retrieval and exchange between authorities, while the EUDI Wallet supports user-controlled holding and presentation of digital credentials. The PoC examines how these synergies can be demonstrated in practice. Figure 1 summarises the two complementary integration patterns.

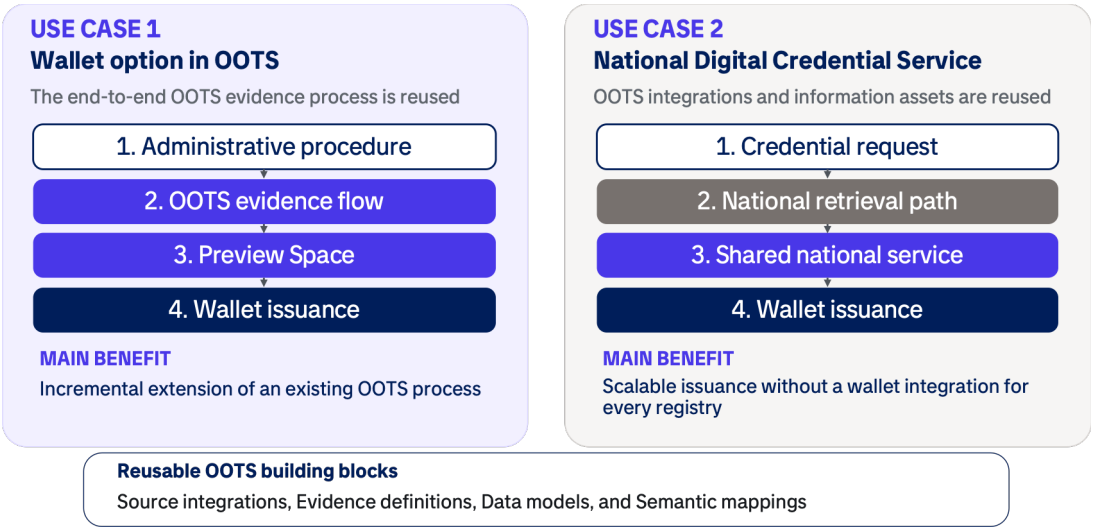


Figure 1 Two Complementary OOTS–EUDI Wallet Integration Patterns Examined in the PoC

4 PoC Architecture and Implementation

4.1 Overall Architecture and Main Components

The PoC architecture combines an OOTS-based evidence exchange model with EUDI Wallet capabilities for issuing and presenting wallet-compatible digital attestations. At a high level, the architecture consists of four main areas: the requester side, the provider side, OOTS Common Services and the EUDI Wallet. Figure 2 presents the overall PoC architecture and the main connections between the OOTS and EUDI Wallet capabilities.

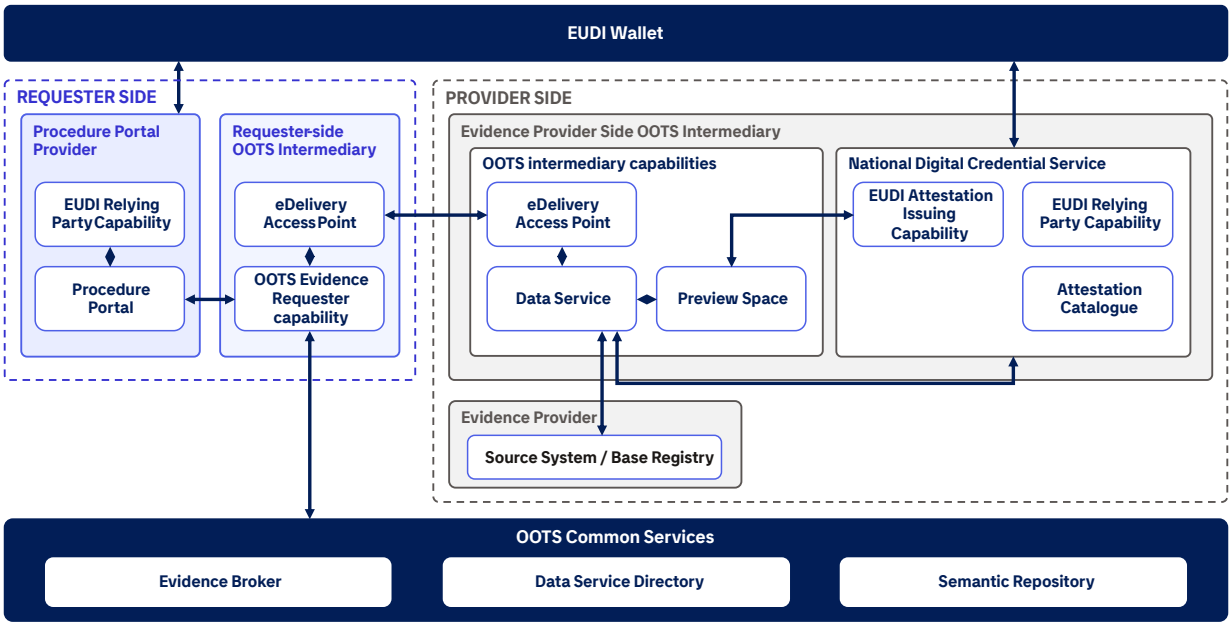


Figure 2 Overall PoC Architecture Connecting OOTS and EUDI Wallet Capabilities

The requester side represents the authority responsible for the user-facing administrative procedure. It includes the Procedure Portal and the EUDI Relying Party Capability used to interact with the user's wallet, for example for wallet-based identification or for receiving information presented from the wallet. The OOTS-specific evidence request is handled through the Requester-side OOTS Intermediary, which includes the OOTS Evidence Requester capability and the requester-side eDelivery Access Point.

The provider side represents the authority and technical capabilities responsible for providing evidence. The Evidence Provider is responsible for the authoritative source data, which is represented in the architecture by the Source System / Base Registry. The Evidence Provider Side OOTS Intermediary provides the OOTS-side technical capabilities needed to serve evidence, including the provider-side eDelivery Access Point, Data Service and Preview Space. The Data Service retrieves or prepares evidence from the source system, while the Preview Space allows the user to review the evidence before it is returned through the OOTS process.

The provider side is also extended with EUDI Wallet capabilities. In the architecture, the National Digital Credential Service provides the service context for wallet-related capabilities, including the EUDI Attestation Issuing Capability, EUDI Relying Party Capability and Attestation Catalogue. This makes it possible to demonstrate how evidence retrieved or prepared through OOTS-related capabilities can also be made available to the user as a wallet-compatible digital attestation. The National Digital Credential Service can support both user-driven attestation issuance and issuance initiated from the OOTS preview

flow. OOTS Common Services support the evidence exchange by helping the requester-side OOTS capability identify the relevant evidence type, data service and semantic resources. These services are shown as a shared European support layer rather than as a direct carrier of personal evidence data. The EUDI Wallet is shown as a user-controlled component that interacts with EUDI relying party and attestation issuing capabilities, but not directly with OOTS Common Services or source systems.

The PoC was implemented in a test setup using the OOTS test environment, test source-system interfaces, a SaaS-based digital identity platform and a test mobile wallet supporting EUDI Wallet-relevant issuance and presentation patterns. The wallet-related parts of the PoC used issuance and presentation flows to issue a proof-of-residence attestation to the mobile wallet and to later present wallet-held information back into a service process.

In the PoC implementation, the logical architecture was realised using several test environments and supporting components:

- KEHA's OOTS 2.0 test environment provided the OOTS-side procedure, OOTS Evidence Requester capability, eDelivery capabilities, Data Service and Preview Space. The Attestation Catalogue was simulated through a user interface in the test environment rather than implemented as a separate production-like component.
- Digital and Population Data Services Agency (DVV) test environment represented the Source System / Base Registry for the proof-of-residence data.
- Tieto SaaS-based digital identity test environment provided the EUDI Relying Party Capability and EUDI Attestation Issuing Capability.
- Test mobile wallet was used to receive the proof-of-residence attestation and later present wallet-held information back into a service process.

In the PoC, data from the DVV register was used because the required integrations were already in place, enabling efficient testing of the concept. In the envisioned operational model, however, credentials would be issued by the relevant national authoritative sources in each Member State. The role of the wallet is to enable the reuse of these nationally issued credentials, including in cross-border interactions where evidence needs to be presented to authorities in another country.

Overall, the PoC architecture demonstrates how OOTS-related capabilities, including source-system integrations, data services, preview functionality and semantic assets, can be extended with EUDI Wallet capabilities. The architecture keeps the OOTS authority-to-authority evidence exchange model in place and adds a user-controlled channel for wallet issuance and later presentation of digital attestations.

4.2 Data Flow and Trust Flow

The PoC demonstrated how evidence can flow through an OOTS-based process and how the same evidence-derived information can also be used in an EUDI Wallet-related process. The data flow can be understood in two complementary parts: first, the OOTS evidence flow, where evidence is retrieved for a specific administrative procedure, and second, the wallet-related flow, where evidence-derived information is issued to the user's wallet and can later be presented by the user in another service process. Figure 3 illustrates the OOTS evidence flow, the wallet-related flow and the trust relationships between them.

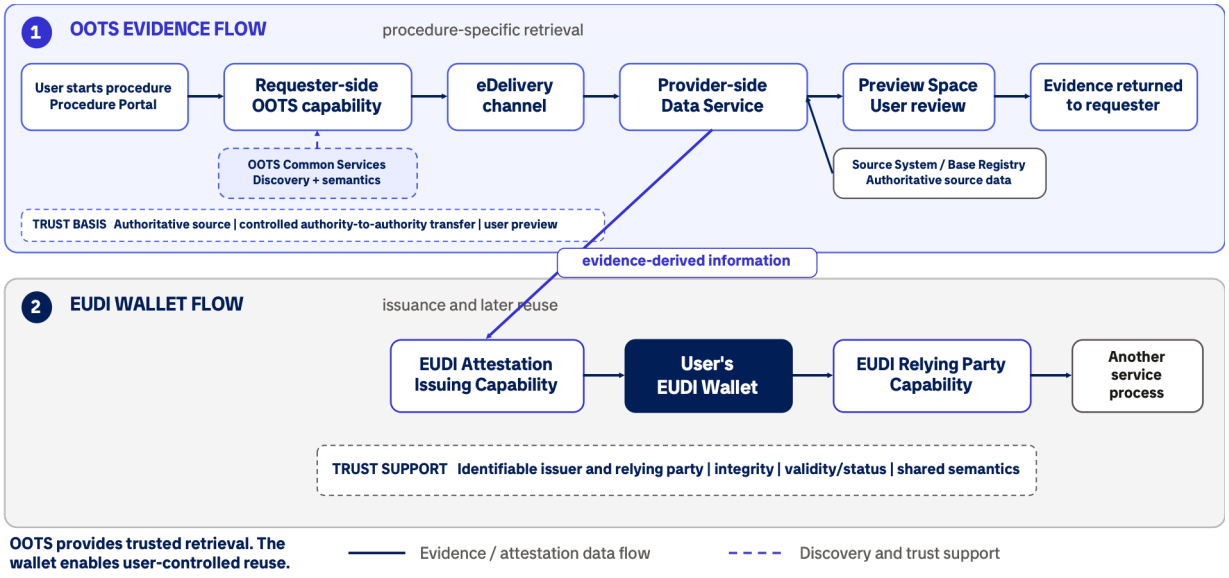


Figure 3 OOTS Evidence Retrieval and EUDI Wallet-Based Reuse

In the OOTS evidence flow, the user starts or continues an administrative procedure through the Procedure Portal. When the procedure requires evidence, the requester-side OOTS capability identifies the required evidence and uses OOTS Common Services to support the discovery of the relevant evidence type, data service and semantic resources. The evidence request is then transmitted through the requester-side eDelivery Access Point to the provider-side eDelivery Access Point.

On the provider side, the Data Service retrieves or prepares the required evidence from the Source System / Base Registry. In the PoC, this concerned proof-of-residence data represented through the Digital and Population Data Services Agency test environment. The evidence is then made available through the Preview Space, where the user can review it before it is returned through the OOTS process. After the preview step, the evidence can be returned to the requester side through the provider-side OOTS Intermediary and the eDelivery channel. If, at a later stage, the OOTS Implementing Regulation is revised and the user journey simplified, for example through the removal of the current mandatory preview functionality, credential material could be provisioned to the wallet via a centralised national OOTS intermediary platform or a "My OOTS Data" service, for which a proof of concept is being developed under the OOTS 2.0 project.

The wallet-related issuance flow builds on this evidence flow. Once evidence has been retrieved and prepared, the same evidence-derived information can be used to create a wallet-compatible digital attestation. In the PoC, this was demonstrated by issuing a proof-of-residence attestation to a test mobile wallet. The wallet-held attestation could later be presented back into a service process through an EUDI Relying Party Capability.

OOTS and the EUDI Wallet create trust in different but complementary ways. In the OOTS flow, trust is based on evidence being retrieved from an authoritative source and transferred through a controlled authority-to-authority process. The requester side relies on evidence retrieved through the OOTS process from the provider side. The user remains involved by requesting the evidence and reviewing it in the Preview Space.

In the EUDI Wallet flow, the trust logic is different. The user holds a digital credential in the wallet and later presents it to another service. The wallet does not make the information authoritative by itself. Trust in the information still comes from the original source data and from the party that issued the attestation to the wallet. The role of the wallet is to let the user receive, hold and present the attestation in a controlled way.

For the receiving service, a wallet-held attestation is a verifiable credential. Trust depends on being able to check who issued it, whether it has remained unchanged, whether it is still valid and what the presented information means.

In a production EUDI Wallet ecosystem, these checks require supporting trust arrangements. Issuers need to be identifiable so that a wallet and a relying service can know who issued the attestation. Relying parties need to be identifiable so that the wallet can show the user who is asking for information. Technical certificates, trust lists or similar mechanisms are used to support this mutual recognition. Schemas and semantic definitions are needed so that the parties interpret the presented information in the same way. Status or revocation mechanisms are needed so that a relying service can check whether an attestation is still valid.

In simple terms, OOTS supports trust in evidence retrieved directly from the original source for a specific procedure. The EUDI Wallet supports trust in a previously issued digital attestation that the user can hold and present later. The two models are therefore complementary: OOTS provides trusted retrieval, while the wallet provides user-controlled reuse.

The PoC demonstrated this relationship at an architectural and technical pattern level. It showed how evidence retrieved from a source system can be transformed into a wallet-compatible attestation, issued to a mobile wallet and later presented back into a service process.

4.3 Wallet Integration in the PoC

The wallet integration in the PoC connected the OOTS-related service flow with wallet-compatible issuance and presentation capabilities. The purpose was to demonstrate, at architecture level, how evidence retrieved or prepared through OOTS-related capabilities could be issued to the user's mobile wallet as a wallet-compatible digital attestation.

The integration covered two main directions. First, evidence-derived information was issued to the user's test mobile wallet. Second, information held in the wallet was later presented back into a service process. These two directions demonstrated both issuance to the wallet and presentation from the wallet.

The integration was implemented between KEHA's OOTS 2.0 test environment, Tieto's SaaS-based digital identity test environment and the test mobile wallet. OOTS 2.0 test environment handled the OOTS-side service flow, evidence retrieval, preview and preparation of the evidence. Tieto's SaaS-based digital identity test environment provided the wallet-facing issuing and relying party capabilities. The test mobile wallet was used by the user to receive and later present the attestation.

In the issuance flow, the handover from the browser-based service flow to the mobile wallet was implemented using a QR-code based mechanism. At a high level, the issuing capability produced a wallet

issuance request, which was made available to the user as a QR code in the service interface. By scanning the QR code with a smartphone, the user could open the issuance flow in the mobile wallet and receive the proof-of-residence attestation. The attestation issued to the wallet was a wallet-compatible representation derived from evidence retrieved from the source-system side. This distinction is important because the PoC demonstrated reuse of OOTS-related evidence capabilities and preparation of evidence-derived information for wallet use.

In the presentation flow, the service process used an EUDI Relying Party Capability to request information from the wallet. The relying party capability generated a wallet presentation request, which was made available to the user as a QR code in the service interface. By scanning the QR code with the mobile device, the user opened the presentation flow in the test mobile wallet, reviewed the requested information and approved the presentation. The wallet-held information was then returned to the relying party side for validation and use in the service process.

This section describes the general wallet integration principles. The detailed implementation of evidence mapping, credential generation, QR-code based delivery to the wallet and later presentation from the wallet are described in sections 5 and 6.

5 Use Case 1: Extending OOTS-Based Evidence Services with Wallet Capabilities

5.1 Integration with the Existing OOTS-Based Evidence Exchange Process

The first use case was built on an existing OOTS-based evidence exchange process. The starting point was a normal administrative procedure in which the user begins the process in a Procedure Portal and the requester side needs proof-of-residence evidence to complete the procedure.

In the baseline OOTS flow, the required evidence is requested from the provider side through the OOTS process. OOTS Common Services support the requester side in identifying the relevant evidence type, evidence provider and data service. The request is then transmitted to the provider side through the OOTS exchange process.

On the provider side, the Data Service retrieves or prepares the requested evidence from the relevant Source System / Base Registry. In the PoC, the source-system role was represented by the Digital and Population Data Services Agency test environment, and the evidence concerned proof-of-residence data.

The key integration point for the wallet extension was the Preview Space. At that point in the process, the evidence had already been retrieved from the national registry to the centralised national Preview Space and could be shown to the user before being returned through the OOTS process. The PoC used this point to add an additional option for the user to receive an evidence-derived digital attestation in a mobile wallet.

This meant that the wallet capability was added alongside the existing OOTS evidence flow. The OOTS process continued to provide the evidence retrieval and preview logic, while the wallet extension demonstrated how the same evidence foundation could also support issuance of a digital attestation to the user.

The following sections describe how this wallet option was implemented: how the proof-of-residence data was prepared for wallet issuance after the user selected the option, how the resulting attestation

was issued to the user's wallet, and how it could later be presented from the wallet back into a service process.

5.2 Adding a Wallet Option to the Preview Space

In the first use case, the wallet extension was introduced in the OOTS Preview Space. Alongside the preview of the retrieved proof-of-residence evidence, the user was offered an additional option to receive a corresponding digital attestation in the mobile wallet. The wallet issuance option added to the OOTS Preview Space is shown in Figure 4.

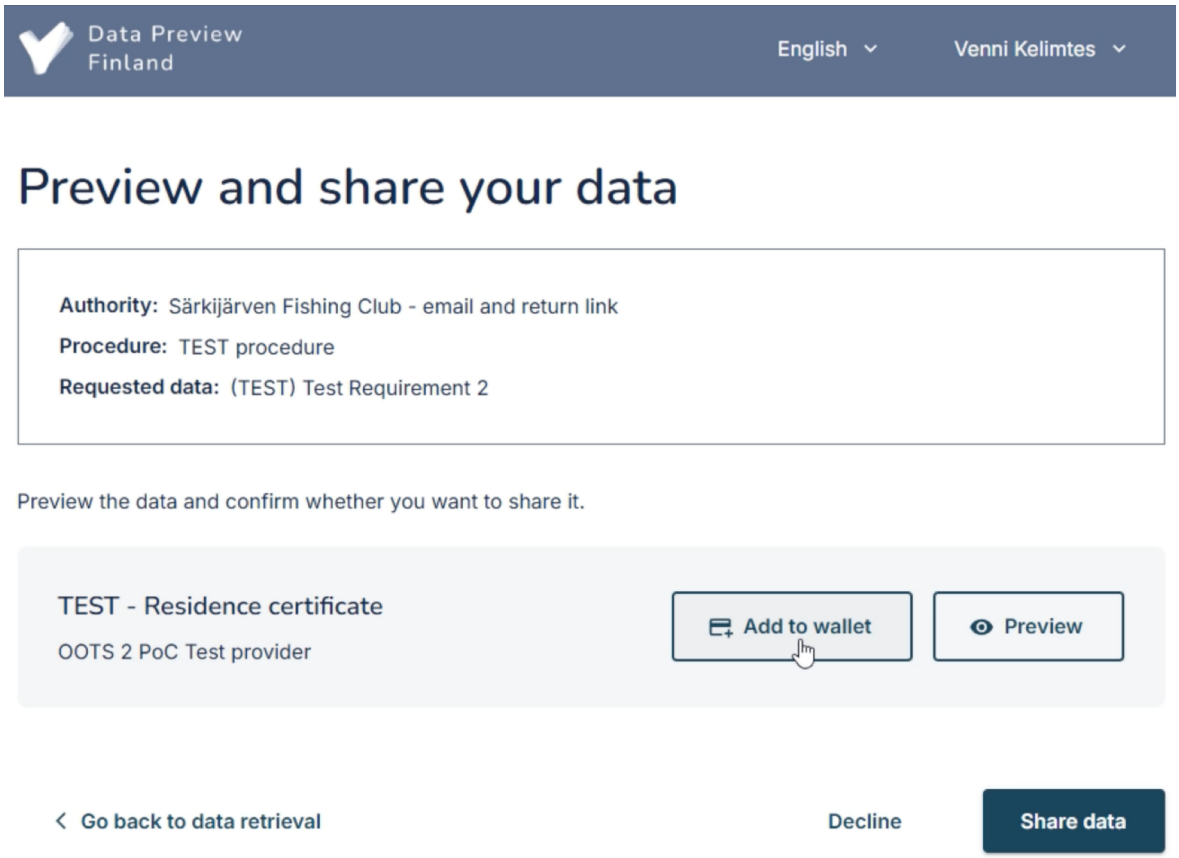


Figure 4 Wallet Issuance Option Added to the OOTS Preview Space in the PoC

The basic OOTS evidence flow remained unchanged. The user could still review the evidence and decide whether it should be used in the requesting procedure. The PoC added a separate wallet issuance path to the same point in the user journey, while keeping the OOTS evidence flow and the wallet issuance flow distinct.

For wallet issuance, the proof-of-residence data had to be converted into a form suitable for issuing a digital credential to an EUDI Wallet. In the PoC, this conversion was carried out in OOTS 2.0 test environment in connection with the Data Service. The proof-of-residence data was mapped to the OOTS proof-of-residence data model published on Finland's Interoperability Platform and expressed in JSON-LD.

The result of this step was prepared attestation data that could be passed to the EUDI Attestation Issuing Capability. The actual issuance interaction with the user's mobile wallet is described in the next section.

5.3 Issuing the Attestation to the User Wallet

After the user had selected the wallet option and the proof-of-residence data had been prepared for issuance, the wallet-facing issuance flow was started. The EUDI Attestation Issuing Capability provided in Tieto's SaaS-based digital identity test environment created the credential offer request URL needed to start the wallet issuance flow. This URL was encoded as a QR code and shown to the user in the Preview Space as part of the added wallet option. Figures 5 and 6 show the credential offer generated in the Preview Space and the subsequent receipt and acceptance of the attestation in the wallet.

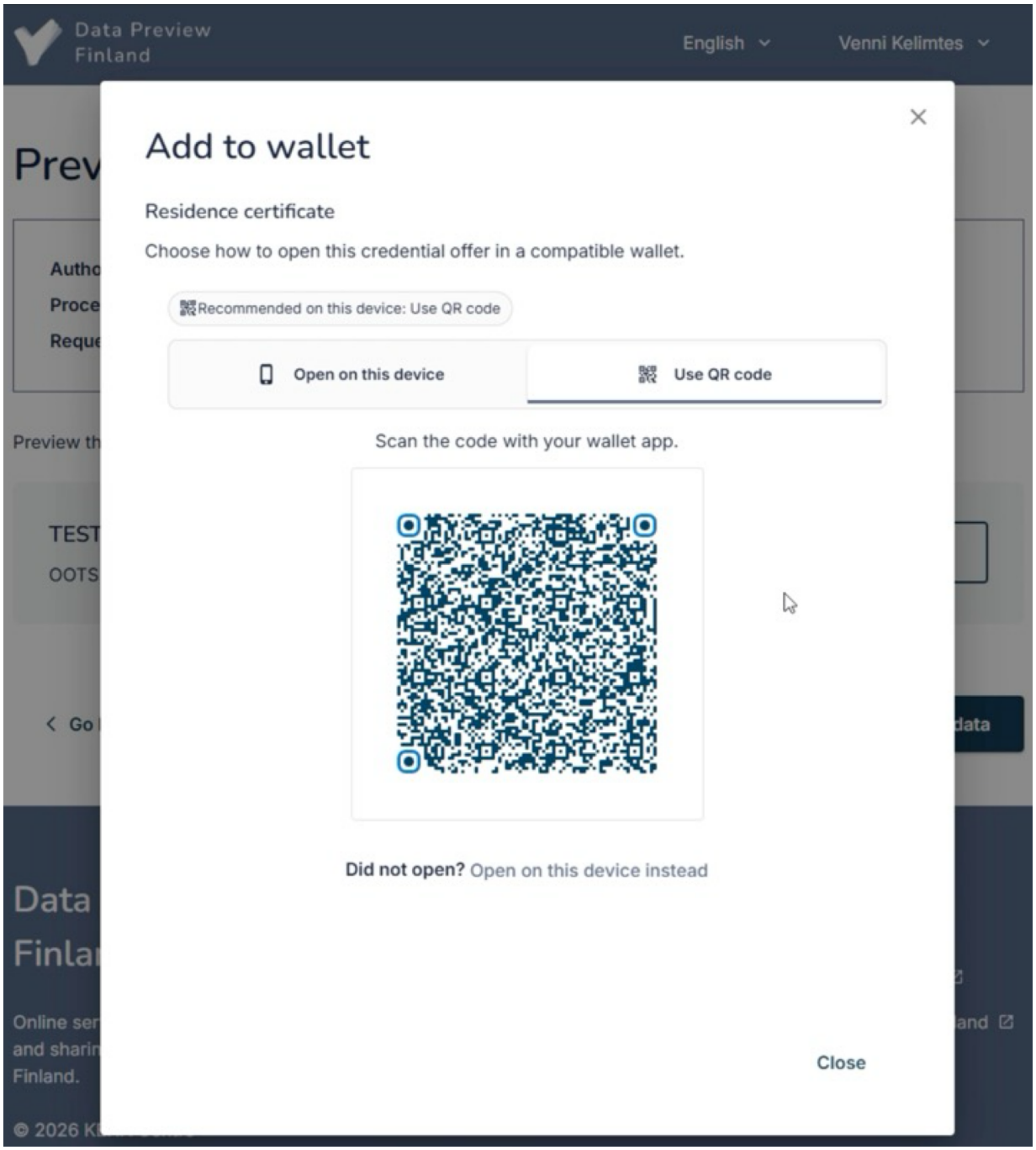
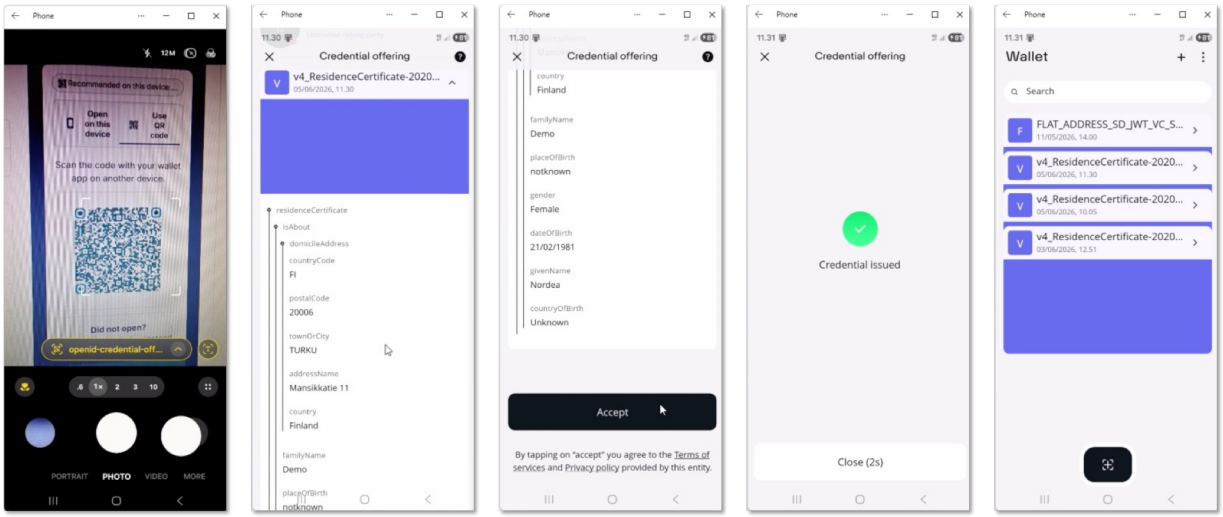


Figure 5 Credential Offer Generated from the OOTS Preview Space in the PoC

By scanning the QR code with a smartphone, the user opened the credential offer in the test mobile wallet and continued the issuance flow on the mobile device. The issuing capability used the prepared attestation data received from the OOTS-side process and issued the corresponding proof-of-residence attestation to the wallet. In the wallet, the user could review the issuance request and accept the proof-of-residence attestation. Once accepted, the attestation was stored in the wallet and could be used later in a presentation flow.



1. User scans the credential offer QR code
2. User reviews the credential details in the EUDI Wallet
3. User accepts the credential in the EUDI Wallet
4. User receives confirmation of successful issuance
5. User can access the credential in the EUDI Wallet

Figure 6 Receipt and Acceptance of the OOTS Evidence-Derived Proof-of-Residence Attestation in the PoC

This step kept the OOTS evidence flow and the wallet issuance flow separate but connected. The OOTS-side process provided the evidence context and the prepared attestation data, while the EUDI Attestation Issuing Capability handled the wallet-facing issuance interaction. The PoC therefore showed that an existing OOTS-based evidence service can act as the business starting point for wallet issuance while delegating the wallet-facing protocol runtime to a dedicated issuing capability.

5.4 Using Wallet-Presented Attestations in OOTS-Related Processes

The PoC also tested the reverse path: how an attestation presented from the wallet could be used in an OOTS-related service process. The implemented example used the proof-of-residence attestation, but the architectural point is broader. A service process can request, and process attestations presented by the user from an EUDI Wallet.

In this part of the flow, the receiving OOTS-related service initiated the request for a wallet presentation. It used the EUDI Relying Party Capability provided in Tieto's SaaS-based digital identity test environment to create a presentation request URL. The URL was then encoded as a QR code and shown to the user in the receiving service. Figures 7-9 show the presentation request, the user's approval in the wallet and the subsequent use of the returned attestation data in the receiving service.

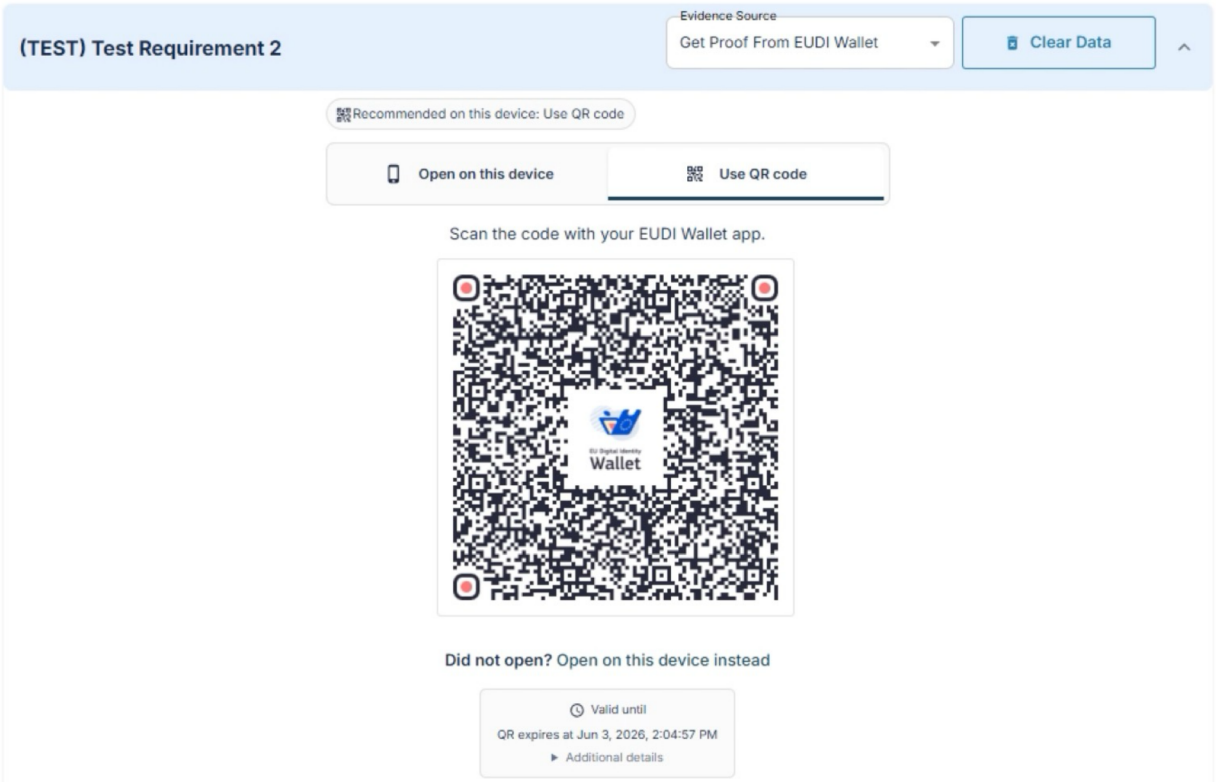
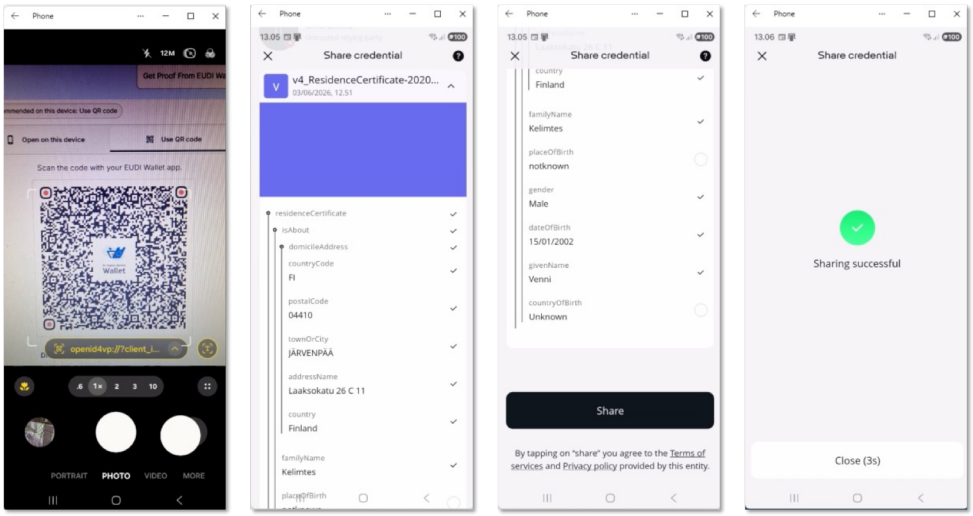


Figure 7 equesting Proof from the User's EUDI Wallet in the Receiving Service in the PoC

By scanning the QR code with a smartphone, the user opened the presentation request in the test mobile wallet. The user could then review what was being requested and approve the presentation of the proof-of-residence attestation. After approval, the wallet returned the requested attestation data through the verification capability.



1. User scans the presentation request QR code
2. User reviews the requested information
3. User approves the presentation
4. User receives confirmation of successful presentation

Figure 8 Presentation of the Proof-of-Residence Attestation from the Test Wallet in the PoC

After the presentation had been received and validated, the returned proof-of-residence attestation data could be mapped into the receiving service's own evidence handling model. This showed how wallet-presented attestations could be used in OOTS-related processes without treating the wallet as a replacement for OOTS evidence exchange.

Figure 9 Wallet-Presented Proof-of-Residence Data Received and Mapped into the Service Process in the PoC

This completed the end-to-end pattern demonstrated in the PoC. Evidence was retrieved from an authoritative source, prepared and issued to the wallet as a digital attestation, and later presented from the wallet into a service process. The national OOTS-side solution remained responsible for the business flow and evidence handling, while the wallet-specific issuance and presentation interactions were handled through dedicated issuer and verifier capabilities.

5.5 Key Findings from the Use Case

EUDI Wallet support can be added to OOTS with limited additional effort. The PoC built on OOTS-side capabilities that are already part of the evidence flow or closely connected to it, including authoritative source data, Data Service, Preview Space, evidence-specific data modelling and structured preparation of evidence data. The wallet-related work was concentrated on the additional capabilities needed to prepare, issue and later present an attestation through the wallet.

The same evidence foundation can support both OOTS and EUDI Wallet use. OOTS provides trusted source context, evidence requirements, data models and service flow. The EUDI Wallet adds a user-controlled channel for receiving an attestation based on the same evidence context and presenting it later in another service process.

Semantic alignment is essential. It ensures that evidence can be understood and used across different actors and service processes, regardless of whether it is exchanged through OOTS or EUDI Wallet infrastructure. OOTS already provides an important starting point for this through the Semantic Repository, Evidence Mapping, data model standardisation and related common services. These elements can support not only OOTS evidence exchange, but also EUDI Wallet issuance, verification and wallet-based presentation when the same evidence structures and semantic descriptions are used across channels.

In the PoC, the link between OOTS evidence data and a wallet attestation was demonstrated with proof-of-residence data. The data was mapped to the OOTS proof-of-residence data model published on Finland's Interoperability Platform and expressed in JSON-LD. This showed how evidence data retrieved

and used in an OOTS context can be prepared for wallet issuance while preserving the meaning and source context of the original evidence.

The shared semantic foundation needs to be developed further. More evidence types need to be modelled in a consistent way and linked to the requirements of receiving procedures. Evidence Mapping, OOTS data model standardisation and shared semantic components such as the Semantic Repository should therefore be developed so that evidence structures, schemas, attributes and source context can be used consistently across OOTS exchange, EUDI Wallet issuance and wallet-based presentation.

Semantic clarity matters for both infrastructures. In OOTS, evidence requesters and providers need a shared understanding of what evidence is required, which source can provide it and how the evidence content relates to the procedure. In EUDI Wallet use, relying parties and receiving services need to understand what a wallet-presented attestation means, which source context it is based on, what claims it contains and how those claims relate to the evidence required in the receiving process. The same semantic foundation therefore supports both OOTS evidence exchange and wallet-based issuance and presentation.

Clear roles make the integration manageable. The OOTS-side service can retain responsibility for the evidence flow, Preview Space, business context and semantic mapping. Dedicated EUDI Attestation Issuing and Relying Party capabilities can handle the wallet-facing issuance and presentation interactions. This division of responsibilities keeps the integration focused and supports a realistic implementation path around existing OOTS infrastructure.

Wallets create a new channel for evidence use. A wallet-presented attestation can be brought into an OOTS-related process and handled in the receiving service's own evidence processing model. This gives public-sector services an additional user-mediated way to use evidence, alongside direct evidence exchange through OOTS.

Scaling requires trust and governance rules. Wider use of EUDI Wallet issuance in OOTS-related processes will require decisions on who is responsible for issuing wallet attestations connected to an OOTS flow and how validity, updates and revocation are handled after issuance. These decisions are needed before wallet issuance can become a predictable extension of OOTS-based evidence services.

The use case indicates a broader path forward. OOTS infrastructure can provide much of the trusted and semantically defined evidence foundation, while EUDI Wallet capabilities can extend the use of that foundation into holder-controlled issuance and presentation. The proof-of-residence example demonstrated the pattern in one evidence domain; broader use depends on applying the same semantic, issuance and trust conditions to other evidence types and service processes.

6 Use Case 2: National Digital Credential Service Based on OOTS Integrations

6.1 National Digital Credential Service

The second use case examined a National Digital Credential Service as a way to accelerate the adoption and use of EUDI Wallets in the Nordic and Baltic member states. Identification is a necessary starting point, but broad everyday use requires attestations that citizens can present, and that public authorities and businesses can rely on, in actual administrative and commercial processes.

Across the Nordic-Baltic region the first EUDI Wallet capabilities are expected to focus on person identification data and a digital identity document. In Finland and some other countries a mobile driving licence is also expected to become part of the wallet-related public-sector credential landscape during this decade, driven by the revised EU driving licence framework. Other public-sector attestations will depend on national prioritisations. These are important starting points, but they create a relatively narrow set of use cases unless they are followed by a broader supply of useful public-sector attestations.

The same concern has been raised more broadly in the Finnish discussion on digital identity. Broad wallet adoption requires a sufficient supply of public-sector attestations that can be used repeatedly across different services. For citizens and businesses, the practical value comes from being able to use verified public-sector information without collecting copies, attachments or PDF documents for each separate process.

The purpose of the National Digital Credential Service is to increase the supply of useful wallet-compatible public-sector attestations. In this use case, the service provides a centralised national access point through which users can request supported public-sector attestations and receive them in their EUDI Wallet. It provides the user-facing service path through which a user can request a supported public-sector attestation, have the underlying data retrieved from national authoritative sources, and receive the resulting wallet-compatible credential.

The use case focuses on national direct retrieval and wallet issuance while reflecting a broader Nordic-Baltic context where similar approaches to digital identity and credential provisioning are emerging. OOTS eDelivery remains the appropriate channel for authority-to-authority evidence exchange in cross-border administrative procedures. The National Digital Credential Service addresses a different service need: it allows authoritative public-sector data to be made available to the user as a wallet-compatible credential for later use supporting interoperability and future cross-border use cases across the Nordic-Baltic region.

The cost and investment rationale is important. A purely authority-by-authority approach would require each authority to acquire or build its own wallet issuance capability and implement the necessary integrations to its source systems. That may be appropriate for some authorities with strong digital service capabilities and high-volume credential needs. As a general model, however, it would make broad availability of public-sector attestations slower and more expensive.

A National Digital Credential Service offers a shared path. The service can build on integrations, evidence definitions and data models already developed for OOTS purposes. This can reduce duplicate integration work, make better use of investments already made in OOTS capabilities and lower the threshold for public-sector authorities to make attestations available to the wallet.

In this model, OOTS-related work provides part of the evidence foundation for wallet-compatible credentials: source-system connectivity, understanding of evidence types, data models and structured preparation of evidence data. The National Digital Credential Service is responsible for the user-facing service flow, evidence selection, source retrieval and preparation of credential data. The wallet-facing issuance interaction can then be handled through a dedicated EUDI Attestation Issuing Capability. This division allows the national service to act as the business starting point for issuance while keeping the wallet protocol runtime as a separate shared capability.

The National Digital Credential Service has a different role from the first use case. The first use case showed how a wallet option can be added to an existing OOTS-based evidence flow at the Preview Space. The second use case examines a broader national service model in which the National Digital

Credential Service provides a shared access point for issuing selected public-sector credentials to EUDI Wallets by using OOTS-related integrations and data models as its foundation.

The broader value of the National Digital Credential Service is practical. It can make the EUDI Wallet more useful for citizens, businesses and service providers, increase the value of existing OOTS investments and allow public-sector authorities to rely on shared issuance and integration capabilities instead of building the same capabilities separately. In Nordic-Baltic region, this also creates opportunities for greater cross-border interoperability and reuse of trusted digital credentials, supporting more seamless interactions between users, service providers and public authorities across national boundaries.

6.2 Reuse of Existing OOTS Integrations

The second use case builds on the work already carried out for national OOTS implementations. OOTS implementation requires public administrations to identify evidence types, determine the authoritative sources that can provide them, define the relevant data structures and build integrations to source systems. The National Digital Credential Service can use this groundwork as a starting point for wallet-compatible public-sector attestations.

The reusable assets are broader than technical interfaces. They include source-system connectivity, evidence definitions, data models, semantic descriptions and the practical knowledge of how source data is retrieved and prepared for use in public-sector service processes. These assets are valuable because the same questions arise when public-sector information is made available as a wallet-compatible credential: which data is needed, which source provides it, how the data should be interpreted and how it can be prepared in a stable structure.

In the PoC, this reuse was examined through the National Digital Credential Service model. The National Digital Credential Service uses existing or OOTS-related source-system integrations to access authoritative public-sector data. It then prepares the data for wallet issuance through a shared national service capability. The source system remains the authoritative source of the data, while the national service provides the user-facing route for obtaining the credential and the preparation logic needed before issuance.

This approach can reduce the need for separate wallet-specific integrations. Without such reuse, each authority that wants to make its data available to the wallet would have to solve many of the same issues separately: source-system access, evidence interpretation, data mapping, credential preparation and connection to an issuing capability. A shared national service can make this work reusable across selected public-sector attestations.

The reuse of OOTS integration assets also supports a more realistic investment path. Public administrations have already invested in OOTS-related integration work, evidence modelling and structured data exchange. Using this work as part of the foundation for wallet-compatible credentials increases the value of those investments and lowers the threshold for authorities to make attestations available through the EUDI Wallet.

The model does require evidence-specific preparation. Source data cannot simply be passed forward as a raw register response. The data has to be selected, structured and mapped into a form that can be issued as a wallet-compatible credential while preserving the meaning and source context of the original evidence. This is why OOTS-related evidence definitions and data models are part of the reusable foundation, alongside the technical integrations.

The reuse model also keeps responsibilities clear. Source systems remain responsible for the authoritative data. The National Digital Credential Service is responsible for the service flow, evidence selection, source retrieval and preparation of credential data. The wallet-facing issuance interaction can be handled through a dedicated EUDI Attestation Issuing Capability. This makes it possible to reuse national evidence capabilities without requiring every source authority to operate the full wallet issuance stack separately. Figure 10 summarises how OOTS-related assets can be reused in the National Digital Credential Service.

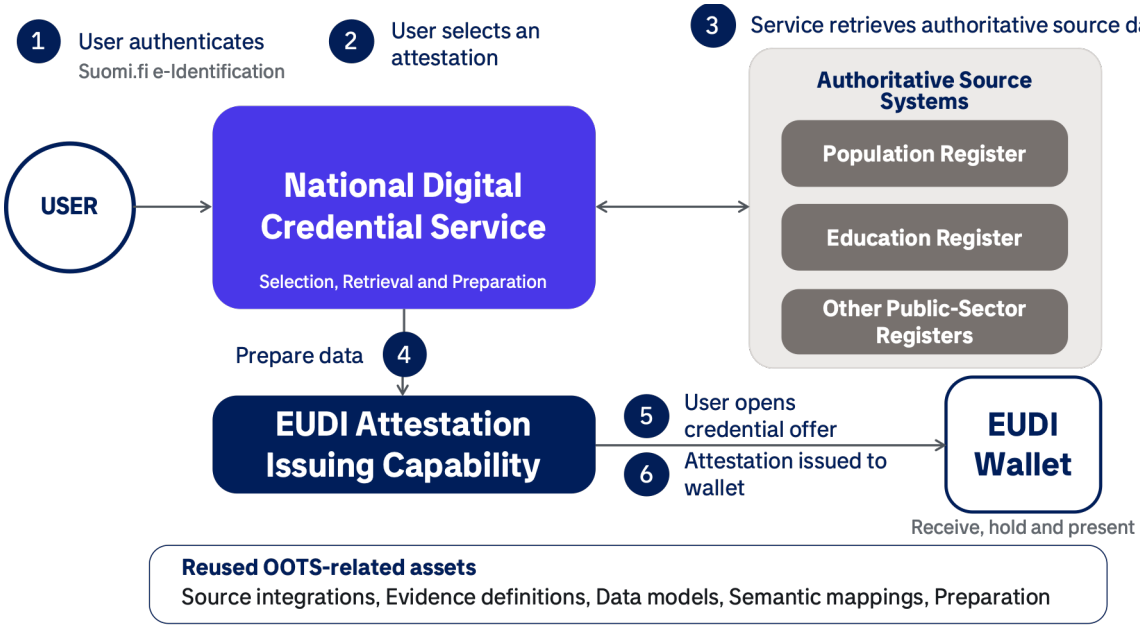


Figure 10 National Digital Credential Service Based on Reused OOTS-Related Assets

This use case therefore treats existing OOTS integration assets as a practical foundation for a broader credential issuance service. The following sections describe how the service architecture is organised, how credential data is retrieved from source systems and how the prepared credential is issued to the user's wallet.

6.3 Retrieval of Credential Data from Source Systems

In the second use case, credential data was retrieved through a national direct retrieval path. The National Digital Credential Service acted as the user-facing entry point. The user entered a protected service flow, selected a supported public-sector attestation and initiated the retrieval of the underlying data from an authoritative national source system. Figures 11 and 12 show the selection of an attestation and the subsequent review and preparation of the retrieved data for wallet issuance.

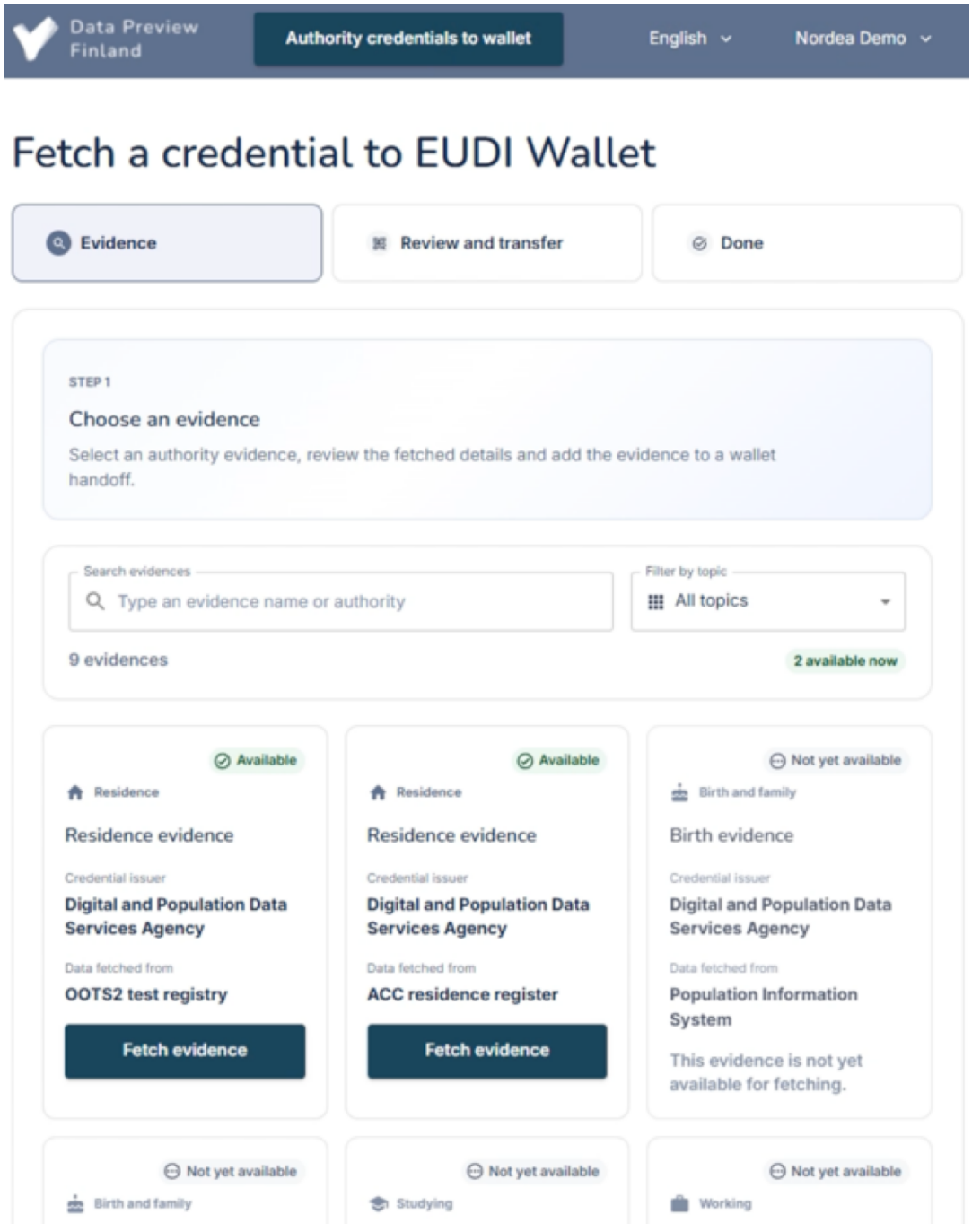


Figure 11 election of a Supported Public-Sector Attestation in the National Digital Credential Service in the PoC

The retrieval step was based on the same principle as OOTS evidence handling: the information must originate from an authoritative public-sector source. In the PoC, this meant using national source-system integrations to retrieve residence-related data from supported national registries and evidence sources. The source system remained the authoritative holder of the original data, while the National Digital Credential Service coordinated the request and prepared the retrieved data for later wallet issuance.

The service first had to validate the selected attestation type and the user context. This included checking that the requested attestation was supported by the service and that the authenticated user context could be used for retrieving the relevant source data. This step is important because the National Digital Credential Service must only retrieve and prepare data for attestations that are supported by the service and allowed under the applicable national rules.

After the source data had been retrieved, it was prepared inside the national service flow. The retrieved response was not treated as a ready-made wallet credential. It had to be structured into a form that could be reviewed and later used for credential issuance. In the PoC, this meant mapping the source response into grouped evidence data for the user-facing service and into a credential payload suitable for the subsequent issuance step.

This preparation step is central to the model. Source systems often expose data in formats that reflect their own internal structures, interfaces and operational needs. A wallet-compatible credential requires a stable structure, clear semantics and a data selection that corresponds to the attestation being issued. The National Digital Credential Service therefore acts as the layer where source data is selected, structured and prepared before it is passed to the issuing capability.

The retrieval path in this use case is national and direct. The purpose is to allow the user to obtain an attestation based on national authoritative data and move it into the wallet. OOTS eDelivery continues to serve authority-to-authority evidence exchange in cross-border administrative procedures. The National Digital Credential Service uses a different retrieval path for a different service situation: user-facing retrieval and preparation of data for wallet issuance.

The PoC demonstrated this retrieval model with residence-related data. The same general approach could be applied to other public-sector attestations if the relevant source-system integrations, data models, access rules and preparation logic are available. Each new attestation type would still require evidence-specific configuration and mapping, because the source data, semantics and service rules differ between evidence types.

The retrieval step therefore forms the link between authoritative public-sector data and wallet-compatible credential issuance. It keeps the source system responsible for the original data, while allowing the National Digital Credential Service to provide a common service path for selecting, retrieving and preparing the data before the wallet-facing issuance interaction begins.

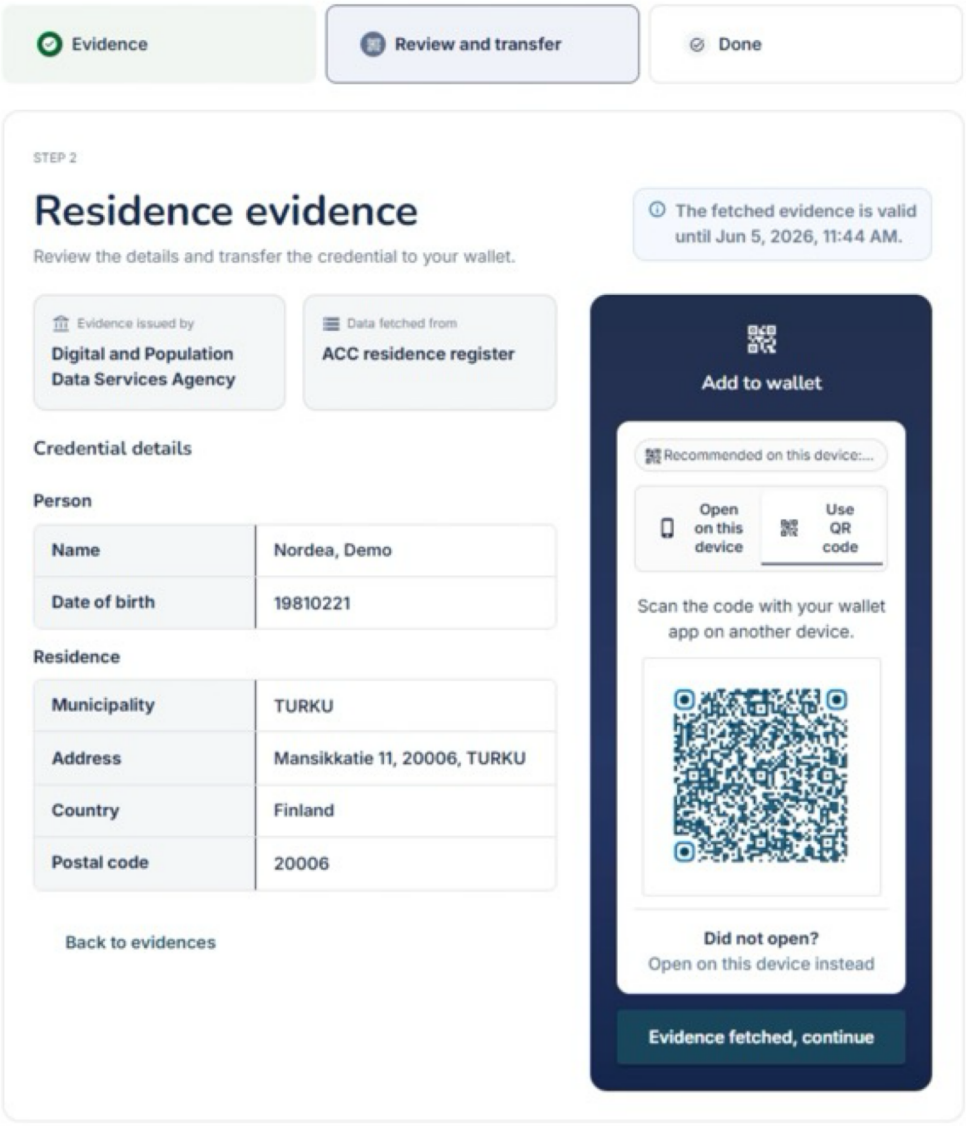


Figure 12 Review of Retrieved Residence Data and Preparation of the Wallet Credential Offer in the PoC

6.4 Issuance of Credential to the Wallet

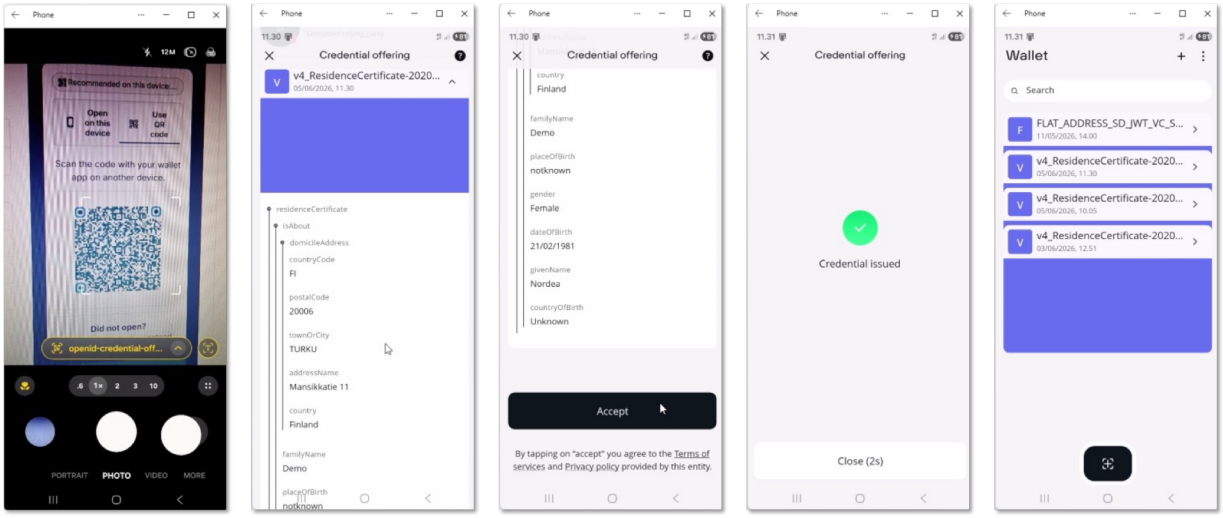
After the relevant source data has been retrieved and prepared, the National Digital Credential Service starts the wallet issuance step. At this point, the data is no longer treated as a source-system response. It has been selected, structured and prepared as credential data that can be used for issuing a wallet-compatible public-sector attestation.

The issuance step begins from the national service context. The National Digital Credential Service provides the business starting point for issuance: it controls the supported attestation type, the user-facing service flow, the source retrieval context and the prepared credential data. The wallet-facing issuance interaction is then handled through a dedicated EUDI Attestation Issuing Capability.

This division of responsibilities is important. The national service remains responsible for the public-sector evidence context and for preparing the credential data. The issuing capability manages the technical interaction with the wallet. In the PoC, this meant that the National Digital Credential Service could start

the wallet issuance flow after the data had been retrieved and prepared, while the issuer capability handled the wallet-compatible issuance runtime.

The issuing capability creates the issuance interaction that allows the user to receive the credential in the wallet. In practice, this can be implemented through a credential offer or a similar wallet-compatible issuance request. The user continues the process in the mobile wallet, reviews the issuance request and accepts the credential. Once accepted, the credential is stored in the wallet and becomes available for later presentation in other service contexts. Figure 13 shows the receipt and acceptance of the resulting proof-of-residence attestation in the wallet.



1. User scans the credential offer QR code
2. User reviews the credential details in the EUDI Wallet
3. User accepts the credential in the EUDI Wallet
4. User receives confirmation of successful issuance
5. User can access the credential in the EUDI Wallet

Figure 13 Receipt and Acceptance of the Proof-of-Residence Attestation Issued through the National Digital Credential Service in the PoC

The credential issued to the wallet represents information derived from an authoritative public-sector source. Its value depends on preserving the link between the issued credential, the source data and the meaning of the original evidence. For this reason, the issuance step relies on the preparation carried out before issuance: data selection, semantic mapping, claim structure and evidence-specific configuration.

The PoC used this model to demonstrate that the National Digital Credential Service can act as the starting point for wallet issuance without each source authority operating the full wallet issuance stack separately. The source authority remains responsible for the underlying authoritative data, while the National Digital Credential Service and the issuing capability together provide a shared path for making selected public-sector attestations available to the user's wallet.

This model also supports the wider purpose of the second use case. If the same issuance approach can be applied to more public-sector attestations, the EUDI Wallet can become more useful without requiring separate wallet-specific issuance implementations for every authority and every source system. The National Digital Credential Service therefore provides a practical route from authoritative public-sector data to wallet-compatible credentials, while keeping evidence preparation and wallet-facing issuance as distinct responsibilities.

6.5 Key Findings from the Use Case

A National Digital Credential Service can increase the supply of useful wallet attestations. The second use case showed how a National Digital Credential Service could provide a practical route for making selected public-sector attestations available to EUDI Wallets. This is important for wallet adoption because the wallet becomes more useful when citizens can present verified public-sector information, and public authorities and businesses can rely on it in real service situations. Building on the interoperability foundations and practical experience gained through Nordic-Baltic OOTS cooperation, this approach can help extend the value of existing cross-border evidence exchange solutions to support the issuance and use of digital credentials in the EUDI Wallet ecosystem. This creates opportunities for greater cross-border interoperability, reuse of common capabilities and more seamless digital services for citizens and businesses operating across the region.

OOTS investments can support wallet issuance. The use case showed that integrations, evidence definitions and data models developed for OOTS purposes can provide a foundation for wallet-compatible public-sector credentials. This can increase the value of OOTS investments by allowing the same groundwork to support both evidence exchange and wallet issuance.

A shared service can reduce authority-by-authority implementation costs. Without a shared national capability, each authority wishing to issue wallet-compatible attestations would need to build or procure its own issuing capability and source-system integrations. A National Digital Credential Service offers a shared route for selected attestations, lowering the threshold for authorities to make their data available to the wallet.

Wallet issuance can be based on direct national source-system retrieval. The use case showed that the National Digital Credential Service can act as a citizen-facing service path for obtaining wallet-compatible attestations based on authoritative national data. In this model, OOTS eDelivery is not used for the evidence retrieval, because the purpose is not cross-border authority-to-authority evidence exchange. Instead, the service retrieves the data directly from national source systems, prepares it for issuance and hands it over to a dedicated issuing capability for wallet-compatible issuance. Once issued to the wallet, these credentials can support cross-border interactions, enabling evidence derived from authoritative national sources to be reused in services across the Nordic-Baltic region and the wider EU, thereby complementing existing OOTS-based interoperability solutions.

The authoritative source remains central. The value of the issued credential depends on the underlying data coming from a trusted public-sector source. In the National Digital Credential Service model, the source system remains responsible for the original data, while the national service handles the user-facing flow, evidence selection, source retrieval and preparation of credential data.

Issuance responsibilities can be separated from source-system responsibilities. The use case supports a model where the national service acts as the business starting point for issuance, while a dedicated EUDI Attestation Issuing Capability handles the wallet-facing issuance interaction. This makes it possible to reuse national evidence capabilities without requiring each source authority to operate the full wallet issuance stack separately.

Evidence preparation remains a necessary step. Source data has to be selected, structured and mapped before it can be issued as a wallet-compatible credential. The PoC therefore confirms the importance of evidence definitions, data models and semantic preparation work. These are part of the reusable foundation created through OOTS-related work.

The model can support broader public-sector adoption of EUDI Wallets. A National Digital Credential Service can help move the wallet beyond identification and a small number of documents by making more useful public-sector attestations available through a shared national capability. This would support citizens and businesses by reducing reliance on copies, attachments and PDF documents in service processes.

The model has Nordic-Baltic scaling potential. The same question is relevant in the whole region and EU: how can countries make authoritative public-sector attestations available to EUDI Wallets without each authority building separate issuance and integration capabilities? If Nordic and Baltic countries can reuse their own OOTS-related integrations, evidence definitions and semantic work, the National Digital Credential Service model could provide a useful reference for wider cooperation.

Scaling requires a clear public-sector issuer mandate. Wider use of the National Digital Credential Service will require a legal and governance model for determining which public-sector body may issue wallet-compatible attestations based on authoritative public-sector source data. In some cases, the issuer may be the authority responsible for the authentic source. In other cases, national legislation or another clear legal basis may be needed to designate another public-sector body to issue attestations on its behalf. The same model should define how validity, updates and revocation are handled after issuance. These arrangements are needed before wallet issuance can become a predictable shared capability for public-sector services.

The current role of national intermediary OOTS platforms would make them natural candidates to operate or coordinate a shared National Digital Credential Services. In that role, such platforms could provide the user-facing service path, reuse OOTS-related integrations and coordinate the preparation of credential data for wallet issuance. The legal issuer of each attestation would still need to be determined separately. It could be the authority responsible for the authentic source, or a public-sector body designated under national law to issue attestations on that authority's behalf. If a national intermediary platform were to act in that latter role, a clear legal mandate would be needed to define the scope of issuance, the source authorities concerned and the handling of validity, updates and revocation. This approach could build on the role already played by intermediary OOTS platforms across the Nordic-Baltic region, supporting the reuse of existing capabilities while enabling future cross-border use of wallet-compatible credentials.

7 Technical Observations

This chapter presents the main technical observations from the PoC and their relevance for further OOTS and EUDI Wallet work.

EUDI Wallet capabilities can be added around existing OOTS evidence flows with limited additional work.

The PoC showed that, where structured OOTS-side evidence data, evidence specifications and data mappings are available, creating a wallet-compatible credential is technically straightforward. The wallet-facing issuance step can then be added at the Preview Space with limited effort and in a technically straightforward way.

From OOTS Evidence Retrieval to Wallet Issuance

Where a National Digital Credential Service acts as the issuer, wallet issuance no longer needs to be closely tied to the current Preview Space. Evidence retrieved through OOTS can be prepared and issued through a National Digital Credential Service, enabling a simpler user journey and reducing reliance on the existing preview functionality. Future regulatory changes could further support this approach by allowing credential material to be provisioned directly to the wallet. **Semantic interoperability is a condition for wider adoption.**

Wallet-compatible public-sector attestations can be used across services only when receiving services can correctly interpret what type of attestation is being presented and what information it contains. This requires common semantic definitions for evidence types, attributes and data structures. Where national definitions differ, the differences need to be mapped explicitly. This is important regardless of the technical channel used for evidence exchange or presentation. The receiving service needs to interpret the evidence consistently whether it is exchanged through OOTS or presented from a wallet. OOTS-related Evidence Mapping, data model standardisation and the Semantic Repository can provide a useful foundation for this work at EU level, because they help define evidence types, attributes, schemas and related semantic resources in a reusable way. Figure 14 summarises the semantic path from authoritative source data to wallet-based presentation and interpretation by the receiving service.

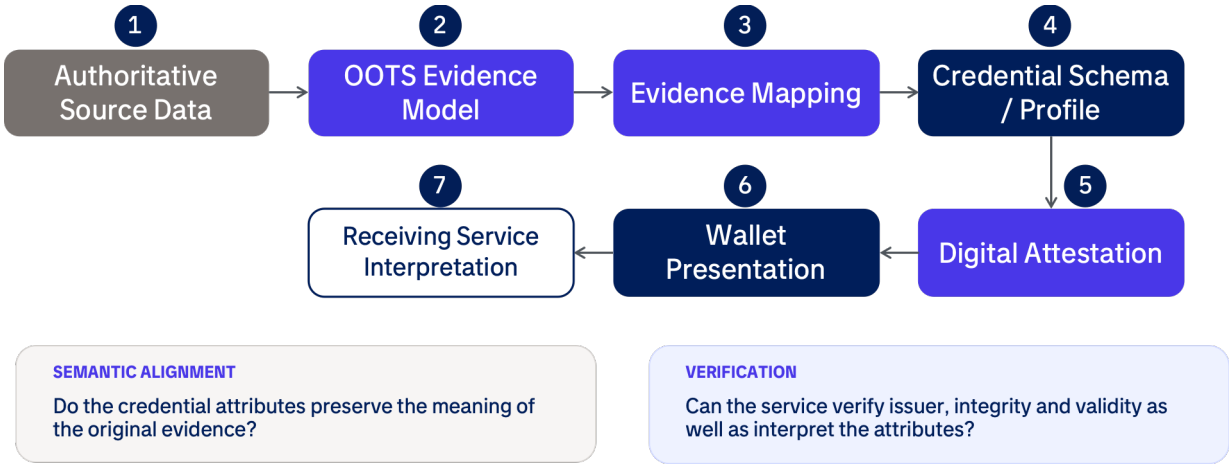


Figure 14 Semantic Alignment from Authoritative Source Data to Wallet-Based Service Use

Existing OOTS-related capabilities can support scalable wallet issuance.

Existing OOTS-related capabilities can make the issuance of new public-sector credentials to EUDI Wallets significantly more straightforward than building a separate wallet-specific implementation for each public-sector register. Registry integrations, evidence handling, data models and service components developed for OOTS purposes can be reused as part of the credential issuance path. New evidence types still require technical configuration, but where the required register data, mappings and credential schema are available, a new credential can be added without implementing an EUDI Wallet integration for each public-sector register.

Cross-border interoperability depends on semantic alignment.

Cross-border use of public-sector credentials requires that receiving services can interpret the presented evidence in the same way across Member States. This depends on common semantic definitions for evidence types, attributes and data structures. Building such definitions for many evidence types across

the EU will take time, because registers, administrative requirements and national data models differ. OOTS-related Evidence Mapping, data model work and the Semantic Repository can provide a practical foundation for this work. Nordic-Baltic cooperation could help move selected evidence areas forward faster by testing common evidence models, mappings and credential profiles in a smaller group of countries before wider EU-level adoption.

Taken together, these observations show that OOTS can become an important accelerator for EUDI Wallet adoption and use. By reusing existing OOTS-related capabilities, public administrations can make a broader range of authoritative public-sector credentials available to EUDI Wallets faster, at lower cost and with limited additional implementation work.

8 Strategic Observations and Next Steps

8.1 OOTS and EUDI Wallet as Complementary Solutions

OOTS can play a strategic role in accelerating EUDI Wallet adoption and use. OOTS already brings together many of the elements needed for useful public-sector credentials, including evidence types, authoritative registers, data models, semantic definitions and integration paths. Reusing this groundwork for EUDI Wallet purposes can help public administrations make more authoritative credentials available to users faster, at lower cost and with less duplicate implementation work.

The value and broad adoption of the EUDI Wallet depend on public-sector credentials being available for everyday use. Strong authentication is a necessary starting point for the wallet, while recurring use depends on whether credentials held in the wallet can be used across various public and private service processes. Residence, education and business register information are examples of trusted public-sector register data that make the wallet more useful for users.

OOTS and the EUDI Wallet should be seen as complementary parts of the same evidence ecosystem. OOTS remains the channel for authority-to-authority evidence exchange where evidence must be retrieved from a public-sector register. The EUDI Wallet adds a user-controlled channel for holding and presenting credentials derived from public-sector register data. OOTS can help broaden the practical role of the EUDI Wallet by making reusable public-sector information available through it.

The next step is to assess which public-sector evidence types already supported in OOTS, or planned for OOTS, are most relevant for everyday wallet use, and in which cases direct registry-based evidence exchange remains the appropriate channel.

8.2 Reuse of OOTS Investments to Reduce Public-Sector EUDI Implementation Costs

Making public-sector credentials available to EUDI Wallets will require capabilities that many authorities do not currently have. If each authority responsible for a public-sector register had to build its own EUDI Wallet integration, the same technical and procurement work would be repeated across the public administration, and the rollout pace would depend on each authority's capacity to fund and implement wallet capabilities.

OOTS investments offer a more sustainable path. Registry integrations, evidence definitions, data models and service components developed for OOTS purposes can be reused as part of an EUDI Wallet integration path. The National Digital Credential Service concept illustrates this principle by using OOTS-related evidence foundations as a basis for making selected public-sector credentials available to EUDI Wallets through a common service capability. In the current public-sector funding environment, reusing

OOTS investments is a more realistic path to broad credential availability than separate authority-specific EUDI Wallet integrations.

The next step is to assess where shared OOTS-related capabilities would reduce duplicate EUDI implementation work most effectively. This should identify which credentials and registers are best suited for a common service model, and where separate authority-specific EUDI Wallet integrations would add value.

8.3 Opportunities for Nordic-Baltic Cooperation

Nordic-Baltic cooperation can help progress selected public-sector credentials through active collaboration. EU-wide semantic alignment across many public-sector credentials will take time, because registers, administrative concepts and data models differ between countries. A smaller group of countries can make progress faster by developing common evidence specifications and testing how evidence could be exchanged through OOTS and used through the EUDI Wallet.

Semantic interoperability is a key condition for this work, especially in cross-border contexts. Public-sector credentials need common or clearly mapped definitions across Member States so that the same evidence can be interpreted consistently in different national contexts. The current challenge is that many evidence types still depend on national concepts, registers and data models, while EU-level catalogues, schemes and semantic assets are still being developed and aligned with OOTS-related semantic work.

This is especially relevant for evidence areas where countries face similar practical questions. Residence, education or guardianship information could be examined through common Nordic-Baltic work to understand which attributes are shared, where national concepts differ and what kind of credential profile would be suitable for wallet use. The aim would be to move selected evidence areas forward through concrete comparison and testing, rather than waiting for all relevant models to mature at EU level.

Nordic-Baltic cooperation can also provide input for wider European interoperability work. Regional cooperation and targeted pilots can produce comparisons, data models, mappings, credential profiles and practical observations that can later support EU-level work. Such pilots could show which attributes are common across countries, where national definitions need explicit mapping, which credential profiles work in more than one national context and which issues need to be addressed in EU-level semantic models.

The next step could be to agree a focused Nordic-Baltic work package for selected evidence areas. The work should compare national concepts and attributes, define common evidence specifications where possible and identify what should be tested through targeted pilots. The results should be documented for use in wider EU-level interoperability work.

8.4 Open Questions for Production Use

The PoC showed that credentials can be issued to the EUDI Wallet based on OOTS-related evidence flows at a proof-of-concept level. The next question is whether the model can be taken forward as a production-ready public-sector service. This requires more than technical integration between OOTS-related evidence capabilities and the EUDI Wallet. The key open questions concern legal basis, issuer role, responsibility allocation, funding, ownership and long-term operation.

A central question is which public-sector actor can issue credentials based on register data and how responsibilities are divided between the register owner, the service handling the evidence flow, the issuer

capability, wallet providers and relying parties. This question arises both when credentials are issued as part of an OOTS-related process and when a shared service model, such as the National Digital Credential Service, is used. In the current situation, these responsibilities may belong to different actors, and the legal and operational basis for issuing credentials on the basis of another authority's register data needs to be clarified.

The operating model also remains open. A shared or integrated credential issuance model requires decisions on ownership and funding. The current challenge is to define who finances the service, who owns it and who operates it. These questions are especially important if the model is expected to serve several authorities and several evidence types rather than a single isolated use case. Table 1 summarises what was demonstrated in the PoC and the additional arrangements required for production use.

Area	Demonstrated in the PoC	Required for production use
Source data	Authoritative test source used	Production registry integration and data-quality arrangements
Credential issuance	Technical issuance demonstrated	Legally mandated issuer and clearly defined responsibilities
Trust	Technical verification pattern demonstrated	Certificates, trust lists and issuer governance
Relying parties	Test relying-party capability used	Registration, identification and access policies
Semantics	Proof-of-residence mapping demonstrated	Governed schemas, profiles and cross-border mappings
Lifecycle	Basic validity handled in the test environment	Status, revocation, updates and expiry arrangements
Operations	PoC components operated for testing	Ownership, funding, monitoring, support and long-term operation

Table 1 From Proof of Concept to Production-Ready Service

The next step is to clarify whether credentials based on public-sector register data can be issued through OOTS-related processes or shared service capabilities under the current legal framework. This should include an assessment of whether national centralised intermediary platforms have a sufficient mandate to issue credentials based on register data, whether legislative changes are needed, and how funding, ownership and long-term operating responsibilities would be arranged.

9 Conclusions

9.1 Summary of the PoC Results

The PoC examined practical synergies between OOTS-related evidence capabilities and the EUDI Wallet. The main conclusion is that these capabilities can reinforce each other. OOTS provides a trusted evidence foundation based on public-sector registers and authority-to-authority evidence exchange. The EUDI Wallet extends the use of that foundation by giving the user a channel to receive, hold and present credentials derived from public-sector register data.

The PoC demonstrated this relationship in two ways. In the OOTS-based use case, wallet issuance was added to an existing evidence flow at the point where the evidence had already been retrieved and made available to the user. This showed that wallet capabilities can be connected to an OOTS-related process without changing the basic role of OOTS as an evidence exchange channel. In the National Digital Credential Service use case, the same reuse logic was examined from a broader service perspective.

OOTS-related integrations, evidence definitions and data models can provide a foundation for making selected public-sector credentials available to EUDI Wallets through a shared service capability.

The most important result is the reuse potential of the OOTS infrastructure. Public administrations do not need to approach every EUDI Wallet credential as a separate implementation starting from each individual register. OOTS-related work already creates much of the groundwork needed for public-sector credentials, including knowledge of evidence types, register sources, data models and semantic definitions. Reusing this groundwork can make credential issuance faster, less costly and easier to repeat across selected evidence types.

This is directly relevant to EUDI Wallet adoption. Strong authentication is an important starting point, but the wallet becomes more valuable when it contains public-sector credentials that users can use in everyday services, such as credentials based on residence or education information. More demanding evidence areas, such as guardianship information, could help test how the model works when legal concepts, lifecycle questions and national differences become more complex.

The PoC also shows where further work is needed. The basic technical connection between OOTS-related evidence capabilities and wallet issuance is manageable, but production use requires decisions on the public-sector issuer role, responsibility allocation, legal basis, funding, ownership and long-term operation. These questions arise both when credentials are issued in connection with an OOTS-related process and when a shared service model such as the National Digital Credential Service is used.

9.2 Long-Term Outlook

The long-term significance of the PoC is that it confirms that OOTS can have a broader role in the EUDI Wallet ecosystem. OOTS is not only relevant as an authority-to-authority evidence exchange infrastructure. OOTS-related capabilities can also help make authoritative public-sector information available for wallet-based use, where this is legally and operationally appropriate.

For countries that have already invested in OOTS implementation, this creates a practical opportunity. Existing evidence work can support more than one channel. The same public-sector evidence foundation can be used for OOTS exchange, for wallet-compatible credential issuance and for later user-controlled presentation from the wallet. This improves the value of OOTS investments and supports a broader public-sector credential supply for citizens.

Nordic-Baltic cooperation is a practical next setting for this work. A smaller group of countries can progress selected evidence areas by developing common evidence specifications and testing how evidence could be exchanged through OOTS and used through the EUDI Wallet. This would allow participating countries to compare national concepts, identify common attributes and document where national mappings are needed before wider European adoption.

The results of this work could also support EU-level interoperability. Targeted Nordic-Baltic pilots can produce concrete material on evidence specifications, national mappings, credential profiles and evidence-specific questions that need to be addressed in European semantic models and attestation-related assets.

The overall conclusion is that OOTS and the EUDI Wallet should be developed as connected parts of the European evidence landscape. OOTS strengthens the trusted evidence base. The EUDI Wallet extends the use of that base into user-controlled credentials. The next phase should focus on turning the PoC pattern into a repeatable and governed model for selected public-sector credentials, while keeping national and Nordic-Baltic work aligned with the emerging European architecture.

10 Glossary and Terminology

This glossary defines the main terms used in this report. The definitions are intended to clarify how the terms are used in the context of the PoC and are not intended to replace formal legal definitions.

Once-Only Technical System (OOTS): The European technical system for exchanging evidence between competent authorities in cross-border administrative procedures under the Single Digital Gateway framework. In this report, OOTS refers both to the European evidence exchange model and to the OOTS-related national capabilities that support evidence retrieval, preview, transmission and data management.

European Digital Identity Wallet (EUDI Wallet): A user-controlled digital wallet provided under the European digital identity framework. In this report, the EUDI Wallet is considered as a channel through which users can receive, hold and present wallet-compatible attestations or credentials based on trusted public-sector information.

Evidence: Official documents or data retrieved from authoritative sources and used in OOTS-related processes. In the OOTS context, evidence is requested for a specific administrative procedure and exchanged through the OOTS evidence flow.

Electronic attestation of attributes / Digital Credential: A wallet-compatible digital attestation of one or more attributes that can be issued to the user's wallet, held by the user and presented to relying parties. This is the more precise regulatory term in the EUDI Wallet and eIDAS context.

Wallet-compatible attestation or credential: An attestation or credential prepared in a form that can be issued to, stored in and presented from an EUDI Wallet. In the PoC, this means that evidence-derived information was mapped and prepared before it was issued to the test mobile wallet.

Holder: The user who receives, holds and presents a wallet-compatible attestation or credential from the EUDI Wallet. In this report, the holder is usually the citizen or user participating in the service process.

Issuer: The party or capability responsible for issuing a wallet-compatible attestation or credential to the user's wallet. In production use, the legal issuer role and mandate must be determined separately from the technical issuing capability.

Relying party: A service or organisation that requests and receives information presented from the user's wallet and decides whether the presented attestation or credential is acceptable for its service process.

EUDI Attestation Issuing Capability: The wallet-facing capability used to create the issuance interaction and issue a wallet-compatible attestation or credential to the user's wallet. In the PoC, this capability was provided through Tieto's SaaS-based digital identity test environment.

EUDI Relying Party Capability: The wallet-facing capability used by a service to request and receive information presented from the user's wallet. In the PoC, this capability was used to demonstrate how a proof-of-residence attestation presented from the wallet could be received and processed in an OOTS-related service process.

National Digital Credential Service: A shared national service model through which users can request supported public-sector attestations and receive them in their EUDI Wallet. In this report, the National Digital Credential Service reuses OOTS-related source-system integrations, evidence definitions and data models, while a dedicated issuing capability handles the wallet-facing issuance interaction.

Authoritative source: The public-sector register, base registry or other trusted source system from which the original evidence or underlying data originates. The trust value of a wallet-compatible attestation depends on preserving the link to the authoritative source and the meaning of the original evidence.

Source System / Base Registry: The system that holds the authoritative data used as the basis for evidence or credential issuance. In the PoC architecture, the Source System / Base Registry represents the origin of proof-of-residence data.

Evidence Provider: The authority or provider-side capability responsible for providing evidence from an authoritative source in the OOTS evidence flow.

Evidence Requester: The requester-side authority or capability that needs evidence for an administrative procedure and initiates the OOTS evidence request.

Data Service: The provider-side OOTS capability that retrieves or prepares evidence from the source system before it is made available through the OOTS process. In the PoC, the Data Service was also relevant for preparing proof-of-residence data for wallet issuance.

Preview Space: The OOTS user-facing preview step where the user can review retrieved evidence before it is returned through the OOTS process. In the first use case, the Preview Space was used as the point where an additional wallet option was added.

OOTS eDelivery: The secure message transport channel used in OOTS for cross-border authority-to-authority evidence exchange. In this report, OOTS eDelivery remains distinct from wallet issuance, which can use national service paths when the purpose is to make an attestation available to the user's wallet.

OOTS Common Services: Common European support services used in the OOTS evidence exchange process, for example to help identify evidence types, data services, evidence providers and semantic resources. In this report, OOTS Common Services are relevant both to evidence exchange and to the possible reuse of OOTS-related assets for wallet-compatible credentials.

Evidence type: A defined category of evidence needed for a procedure or credential use case. Evidence types help determine what information is required, which source can provide it and how it should be structured.

Semantic interoperability: The ability of different systems and organisations to understand evidence, attributes and credentials in the same way. In this report, semantic interoperability is a condition for scaling both OOTS evidence exchange and EUDI Wallet-based issuance and presentation.

Evidence Mapping: The work of mapping procedural evidence requirements, evidence types, source data and semantic definitions so that evidence can be requested, provided, issued or interpreted consistently across services.

Semantic Repository: A shared semantic resource used in the OOTS context to support common understanding of evidence types, attributes, schemas and related semantic assets.

Credential schema or credential profile: The defined structure and semantics of a wallet-compatible credential. A credential schema or profile determines which claims are included, how they are represented and how receiving services can interpret them.

Lifecycle, validity and revocation: The mechanisms and responsibilities related to whether an issued attestation or credential remains valid after issuance, how its status can be checked, and how it can be revoked or updated if necessary. These questions were not resolved by the PoC and remain part of the production operating model.

- ENDS -