Dissemination level: Public

D3.1: List of available compliant wallets in EWC and documentation

WP3

Authors: LCubed AB (iGrant.io), Sweden (Ms. Lotta Lundin, Mr. Lal Chandran)
Contributors: Ricky Thiermann (Spherity)

Reviewers: Andriana Prentza (UPRC), Esther Makaay (Signicat) 1 Nikos Triantafyllou (UAegean)

Day of submission: 27 July 2025

Co-funded by the European Union

Revisions

Version	Date	Author	Changes
1.0	18-July-2025	Lal Chandran / Lotta Lundin, iGrant.io	WIP, Ready for content review

Co-funded by the European Union

Table of Contents

Co-funded by the European Union

Co-funded by the European Union

Executive Summary

This deliverable outlines the results of Task 3.1, “Wallet provisioning”, and provides a comprehensive overview of the multiple wallet solutions developed within the European Wallet Consortium (EWC). These solutions have been verified and validated for use in the EWC Large Scale Pilot use case scenarios.

Through a structured and transparent Request For Comments (RFC) process, EWC has established a clear, prescriptive stance, providing interfaces and guidelines that align with the identified requirements, including legal, architectural framework (ARF), and EWC use cases. This has enabled wallet providers, both for natural and legal persons, to implement their solutions, interoperating and proving conformance through the EWC Interoperability Test Bed (ITB). The core of this document is an up-to-date list of RFC-compliant wallets as of EWC Phase 03, covering:

- Natural Person Wallets
- Legal Person Wallets or Business Wallets
- Issuer-only and Verifier-only implementations

Each solution has been tested against a defined set of RFCs relevant to its role (e.g., issuance, wallet unit holder functions, and verification) and validated within the context of EWC's Large-Scale Pilot (LSP) scenarios. This deliverable is a reference point for the current state of EWC RFC-compliant wallets. It also showcases the EWC approach as a scalable framework that drives a multi-provider, interoperable EUDI Wallet ecosystem, rooted in transparency, collaboration, and compliance in a continuous manner. It is strongly recommended that this approach be adopted on a longer-term basis, with the ITB being continuously maintained and updated to reflect evolving technical and standards requirements, security expectations, and regulatory changes, ensuring it remains a vital enabler of a trusted and future-ready EUDI ecosystem.

Co-funded by the European Union

List of Abbreviations

ARF	Architecture and Reference Framework
EUDI	EU Digital Identity
EWC	EU Digital Identity Wallet Consortium
HAIP	High Assurance Interoperability Profile
ISO/IET	International Organisation for Standardisation
LPID	Legal Person Identification Data
LSP	Large Scale Pilot
mdoc	Mobile Document
mDL	Mobile Driver's License
OpenID4VCI	OpenID for Verifiable Credential Issuance
OpenID4VP	OpenID for Verifiable Presentations
PID	Personal Identification Data
(Q)EAA	(Qualified) Electronic Attribute Attestation
RFC	Request for Comments
RP	Relying Party
RQESP	Remote Qualified Electronic Signature Provider
SCA	Strong Customer Authentication
SD-JWT	Selective Disclosure JSON Web Token
TL	Trust List
WCC	Wallet Core Component
WP	Wallet Provider
WP	Work Package
WS	Wallet Solution
WU	Wallet Units
WUA	Wallet Unit Attestation
W3C	World Wide Web Consortium

Co-funded by the European Union

1. Introduction

1.1 EWC approach to Large-Scale Pilot use cases

This diagram illustrates the ecosystem of the European Wallet Consortium (EWC) Large Scale Pilot (LSP). It explains why Request for Comments (RFCs) have become necessary to ensure cohesion and interoperability.

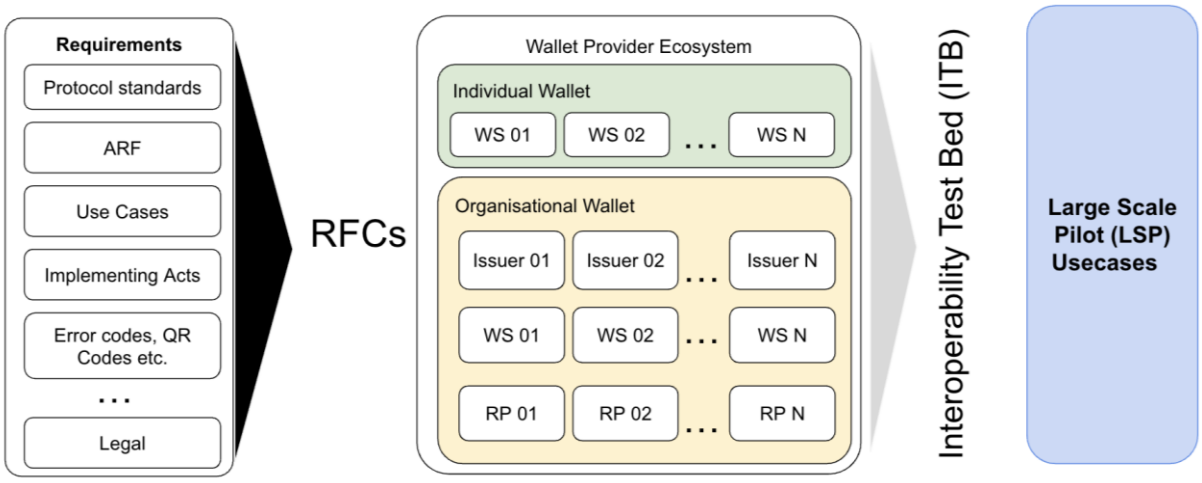

Figure 1: EWC approach to the Large-Scale Pilot use cases

On the far right, the LSP use cases represent real-world scenarios involving various entities, including issuers, verifiers (relying parties), wallet providers, and other relevant parties. Each actor may bring their interpretations, implementations, or extensions of standards. This results in:

- A large number of possible combinations of entities.
- Interoperability challenges arise when each party interprets the specifications differently or prioritises one aspect of the support over another.
- Complexity in scaling and testing all these combinations reliably.

1.2 The challenge: Fragmentation without clear guidance

Without clear, opinionated guidance, each participant (Issuer, RP, Wallet Software) might implement:

- Different behaviours for credential issuance and verification.
- Diverse interpretations of protocol standards.
- Variations in handling legal, technical, and UI/UX aspects.

This fragmentation would lead to:

- Incompatibilities between wallets and services.

Co-funded by the European Union

- Increased cost of testing and integration.
- Difficulty in reaching consensus on shared success criteria in the test bed (ITB).

1.3 RFCs: Consensus-based specifications with prescriptive guidance

RFCs were introduced to address the challenges and to bridge the gap between aligning the requirements from LSP use cases, the ARF [1], standards, and specifications, thereby enabling an interoperable ecosystem of wallet providers, issuers and relying parties. RFCs [2] are curated, EWC community-reviewed documents that define a clear, prescriptive, and common way of implementing EUDI wallet interfaces for ecosystem participants, specifically regarding Issuer, Wallet Unit (WU), and Relying Party (RP) functionalities. The EWC RFCs are formulated based on the following:

- Protocol standards (e.g., OpenID4VCI, OpenID4VP, W3C VC, W3C Presentation Protocol, SD-JWT, mdoc/mDL formats, etc.)
- The EU ARF (Architecture Reference Framework) [1]
- Profiles for different roles (e.g., what an organisational wallet must support)
- Implementation details (e.g., QR formats, error codes)
- Use case definitions coming from WP2 and WP3
- Legal and compliance guidance (E.g. EU Regulation 2024/1183, Implementing Regulations, etc.)

These are then distilled into practical test cases within the ITB.

2. EWC RFC process for compliance

This diagram illustrates the EWC RFC lifecycle and its execution across the work packages (WP3, WP4, and WP2) within the European Wallet Consortium (EWC) framework.

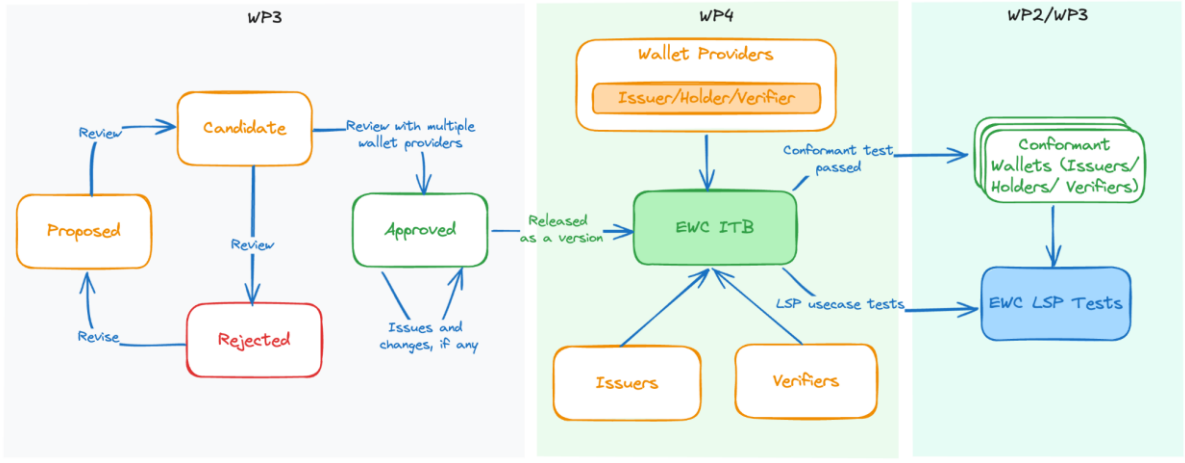

Figure 2: EWC cross-work package process

Co-funded by the European Union

The subchapters below provide a detailed explanation of each element illustrated in the diagram.

2.1 WP3: RFC development process

The left section shows the **RFC authoring and governance** flow managed within **WP3**:

1. **Proposed** – An RFC begins as a proposal. It can come from experience, gaps observed in standards, or the needs of LSPs.

2. **Candidate** – Once drafted, it undergoes a review process, often with input from multiple wallet providers.

3. **Approved** – After sufficient review and alignment, an RFC is approved and:

    - Released as a version.

    - Fed into the EWC Interoperability Test Bed (ITB) as test cases.

4. **Rejected** – If the RFC fails review or lacks consensus, it is rejected and optionally revised for resubmission.

As reflected in the EWC RFCs, to contain the scope within the EWC ecosystem, the following choices, in summary, are made [Ref: Appendix B]:

- Credential formats: IETF SD-JWT (Mandatory) and, optionally, W3C VC (JWT) and ISO 18013-5 (mdoc/ mDL)

- Data workflow spec: OpenID4VCI Draft 15 (ID2) and OpenID4VP Draft 23 (ID3)

- Digital Credentials (DC) APIs are optional in EWC Ph. 03 (EWC RFC Release v3.0).

2.2 WP4: Conformance & ITB testing

The middle section shows the **interplay between wallet providers and the ITB**, primarily under **WP4**:

- Wallet Providers implement RFCs in their software for roles such as Issuer, Holder, and Verifier.

- These implementations are tested in the EWC Interoperability Test Bed (ITB) to ensure they conform to the RFC requirements.

    - **Conformance test passed** → The wallet or actor is marked as compliant.

- Conformant wallets can then participate in actual use case testing.

Co-funded by the European Union

- The ITB ensures that only implementations following approved RFCs are allowed to participate.

For the final details on the interoperability outcome on wallet implementation, refer to EWC D4.3 [4].

2.3 WP2/WP3: LSP use cases

The rightmost section links the outcomes of WP3 and WP4 to WP2, where real LSP use cases are tested:

- Only conformant wallets (Issuer, Holder, and Verifier) are used to test real-life scenarios in LSPs.
- EWC LSP tests validate technical conformance and whether implementations perform well in specific use cases.

This loop ensures:

- All participating entities use standardised, well-tested building blocks (RFCs).
- Implementation quality is high.
- LSP results are reliable and repeatable.

3. Requirements towards Business Wallets or Legal Person Wallets

The EU Architecture Reference Framework (ARF) [1] was initially developed with a natural person wallet in mind. Early in the EWC LSP, it became evident that the needs of legal entities were not adequately addressed, starting with the issuance of LPIDs. This distinction between business wallets (synonymous with “legal person wallet”) and natural person wallets, therefore, had to be clearly articulated before proceeding with the detailed implementation requirements.

Legal person wallets often require integration with internal enterprise systems and are typically deployed in server-based environments, with minimal end-user interaction. These differences were captured and aligned in the EWC Legal Person Wallet Definition Document [3], which served as the foundation for the requirements outlined below.

Form factor: Legal person wallets are frequently deployed in server environments, such as on-premises or in cloud-based infrastructures, often without a GUI. Natural person wallets typically operate on mobile devices with a user-facing GUI.

Automation: Legal person wallets are designed for automated operations, enabling seamless interaction without requiring end-user involvement. Natural person wallets rely heavily on the end user for credential management.

Co-funded by the European Union

Complexity of use cases: Legal persons may need to integrate their internal systems and processes with the wallet, such as enterprise resource planning systems and customer relationship management systems. Natural person wallets are primarily used for managing individual credentials.

Credential management and presentation: The ability to store, manage and selectively present credentials is a core feature. Legal persons must control which credentials are shared with external parties while ensuring compliance with regulatory requirements.

Issuer and relying party functionality: Each organisational wallet must support both issuer and relying party functions, enabling the issuance and verification of credentials.

Wallet core component (WCC): The wallet must support essential functions, including communication between different wallet instances and the automated exchange of credentials.

Cloud integration: Legal person wallets must be deployable in flexible environments, supporting both on-premises and cloud-based installations. This is important for organisations that need scalable enterprise-level solutions that integrate with existing systems and infrastructure.

Interoperability and standards compliance: The wallet must comply with key standards and protocols outlined in the implementing acts, ensuring seamless operation with other wallets and systems across borders.

Security and encryption: Security is paramount. The wallet must implement strong encryption for both the storage and communication of credentials, in line with industry standards, to protect organisational data.

To assess the features of wallet providers in the EWC that meet each of these requirements, Task Group 3.1.2 conducted a survey. The results of this survey are available in Appendix A. A more detailed explanation of each wallet can be found in EWC Deliverable D3.2.

4. List of RFCs

The following table summarises the list of RFCs created during the project to build the EWC Wallet Ecosystem, which consists of Issuers, Wallet Units, and Relying Parties. These are published on the EWC RFC GitHub [2] and depict the status as of July 2025.

RFC #	RFC Title
RFC-001	Issue Verifiable Credential - v3.0 prescribes the interactions through which an issuer provides verifiable credentials to a holder's wallet using OpenID4VCI, supporting both authorisation-code and pre-authorised flows on the same device or across devices. It defines how credential offers, access tokens and credential endpoints are used to enable secure and interoperable issuance. The RFC also outlines holder-binding methods,

Co-funded by the European Union

	such as cryptographic or biometric proof, to ensure that the credentials are bound to the legitimate holder.
RFC-002	The Present Verifiable Credentials Workflow - v3.0 prescribes the interactions through which a holder presents verifiable credentials to a verifier using OpenID4VP, supporting both same-device and cross-device flows. It defines how presentation requests, VP tokens and presentation definitions are exchanged to enable structured and interoperable processes. The RFC also outlines holder-binding methods, such as cryptographic or biometric proof, to verify legitimate possession of the credentials.
RFC-003	Issue Person Identification Data (PID) - v2.1 prescribes the end-to-end interactions whereby a Member State-approved identity provider issues official personal identification data to a wallet using an OAuth-based OpenID4VCI flow. It standardises how PID providers authenticate the holder, present PID offers, exchange access tokens and issue credentials, enabling secure issuance of harmonised PID datasets (for natural or legal persons) to interoperable wallets. The RFC also outlines holder-binding mechanisms, metadata publication, and compliance with eIDAS LoA requirements to ensure trusted and privacy-preserving identity provisioning.
RFC-004	Individual Wallet Unit Attestation - v1.0 prescribes the interactions by which a wallet instance obtains a Wallet Unit Attestation (WUA) from its Wallet Provider. It defines a protocol where the wallet sends device and instance data (such as hardware identifiers, secure element status, and cryptographic keys), and in return receives a signed attestation asserting the wallet instance's authenticity and compliance. This ensures verifiers and issuers can trust that they are interacting with a genuine, certified EUDI Wallet instance.
RFC-005	Issue Legal Person Identification Data (LPID) - v1.0 prescribes the end-to-end interactions through which a Member State-approved identity provider issues LPID to an organisation's wallet using an OAuth-based OpenID4VCI flow. It standardises how issuers authenticate organisational holders, present LPID offers (in-time or deferred), exchange access tokens, and deliver credentials containing harmonised data, such as the legal name and unique legal-entity identifier. The RFC also defines holder-binding methods, metadata publication, and compliance with eIDAS/LPID rulebook requirements to ensure trusted, interoperable organisational digital identities across the EUDI ecosystem
RFC-006	Organisational Wallet Unit Attestation - v1.0 prescribes the interactions by which a wallet instance for an organisation obtains a WUA from its WP. It defines how the organisational wallet transmits instance and hardware data, such as secure element status, cryptographic keys, and device identifiers, to its provider and receives a digitally signed attestation asserting compliance, authenticity, and secure cryptographic binding. This ensures issuers and verifiers can trust they're communicating with a genuine, certified organisational EUDI WU according to EWC standards.
RFC-007	Payment Wallet Attestation - v1.1 prescribes the interactions through which a payment-capable EUDI wallet instance obtains an SCA-compliant

	attestation from its provider, allowing integration with banks and payment services. It standardises how the wallet shares device, secure-element, and cryptographic key information via OpenID4VCI, and how it receives a signed attestation asserting compliance, authenticity, and binding to the wallet instance. This ensures payment service providers and verifiers can trust the wallet's integrity and SCA readiness within the secure EU digital payments ecosystem.
RFC-008	Payment Data Confirmation - v1.0 prescribes the interactions where a wallet confirms user-approved payment data with a relying party using OpenID4VP, embedding cryptographically-signed transaction details to prove explicit consent. It standardises how payment request definitions, payment transaction payloads, key-binding JWTs, and SD-JWT attestations are exchanged between the merchant, wallet, and verifier to ensure structured, interoperable, and tamper-evident confirmation of payment intent. By anchoring the transaction within the holder's verifiable presentation, it enhances trust, reliability and SCA compliance in the EU payment ecosystem.
RFC-010	Document Signing using Long-Term Certificates - v1.1 prescribes the interactions whereby a wallet performs qualified electronic signing of documents using long-term qualified certificates via a Remote Qualified Electronic Signature Provider (RQESP). It defines how the wallet, leveraging a holder's PID-derived certificate, authenticates with the service, engages in a signing protocol with challenge and response, and obtains a secure signature created on a remote signing device compliant with QES standards. The RFC ensures that signatures are based on eIDAS and Cloud Signature Consortium rules, are securely timestamped, and are verifiable for long-term preservation.
RFC-011	Payments with Verifiable Receipts - v1.0 prescribes the protocol through which a wallet obtains a cryptographically verifiable proof of payment receipt from a merchant as a verifiable credential, leveraging OpenID4VP flows. It standardises how the merchant issues a receipt credential containing transaction details (amount, time, merchant ID), the wallet presents it, and the verifier confirms authenticity. This enables users and relying parties to verify completed payments with tamper-evident, interoperable receipts across the EUDI ecosystem.
RFC-012	Trust Mechanism - v1.0 prescribes how wallet providers, issuers and verifiers establish trust in the EUDI Wallet ecosystem using the EU Trust List and ETSI TS 119 612 standards. It defines structured and interoperable interactions anchored in eIDAS 1.0 and its subsequent amendments to verify participants, their credentials and attestation status. By relying on a trusted list infrastructure, all ecosystem actors can reliably authenticate issuers, wallet instances and verifiers across Member States.
RFC-013	Issue PhotoID - v2.0 prescribes the interactions through which a Member State-approved issuer provides a digital Photo ID credential, conforming to ISO or IEC TS 23220-4, to a user's wallet using an OpenID4VCI flow. It sets out how the holder authenticates, receives a Photo ID offer, exchanges access tokens, and securely obtains the issued photo credential. The RFC ensures that the process for issuing a Photo ID is consistent and interoperable within the EUDI ecosystem.

RFC-100	EWC Interoperability Profile Towards ITB - v2.0 prescribes the standards and configurations that EUDI wallet providers, issuers and verifiers must follow and validate through the EWC Interoperability Test Bed. It defines the required protocols, data formats, security measures and conformance profiles to ensure consistent and cross-border interoperability. The RFC also outlines the ITB process itself, describing how solutions are tested, validated, and certified within the EWC framework. A summary of key technological choices is given in Appendix B.

Table 01: List of EWC RFCs approved during the EWC LSP project

5. EWC compliant Wallet Solutions

The figure below illustrates the progress of the RFC process and outcomes across three phases of the EWC LSP. It shows how the consortium has refined its specifications through a structured RFC process with increasing participation over time.

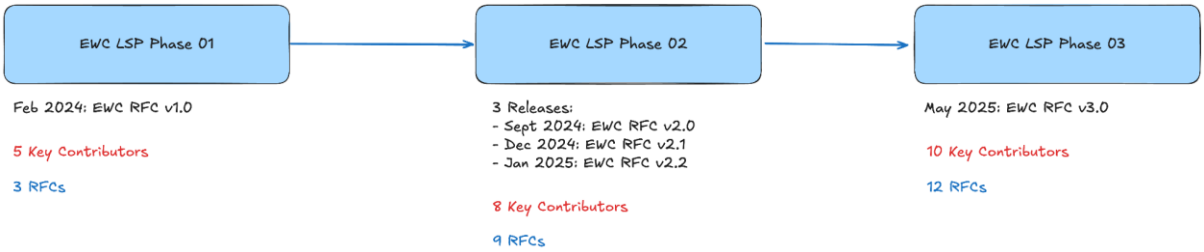

Figure 03: EWC RFCs process through the LSP phases

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

5.1 Natural Person Wallet Solutions

The following are the Natural Person Wallet Solutions, compiled by the EWC RFCs and tested against the ITB. The status is for **EWC Phase 03** LSP tests (Dated: July 2025)

Wallet	App Link	RFC001	002	003	004	005	006	007	008	010	011	012	013	100
iGrant.io - Data Wallet	iOS, Android	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
Lissi ID-Wallet	iOS, Android	✅	✅	✅	✅			✅	✅	✅		✅	✅	✅
Validated ID	iOS, Android	✅	✅	✅		✅				✅		✅		✅
Digidentity	[N/A]	✅	✅	✅	✅					✅		✅	✅	✅
E-Group MyD	[N/A]	✅	✅	✅						✅				✅
SE - DIGG	[N/A]	✅	✅	✅	✅									✅
Identity Consortium	[N/A]	✅	✅	✅						✅				

Table 02: List of Natural Person Wallet Solutions compliant with EWC RFCs

Co-funded by the European Union

Some of the above wallets that were made available in any of the EWC LSP phases are described in detail in the subchapter below. Many of these wallets not only contributed to formulating the interfaces but also updated their solutions based on the finalised RFC.

5.1.1 iGrant.io Data Wallet

LSP Contributions	Led the EWC ecosystem enabler track and contributed as primary author or reviewer of EWC RFCs [2]. Additionally, contributed to open-sourced SDKs for the Android and iOS software stack and actively participated in the development of the EWC ITB.		
Platform Support	iOS: Yes	Android: Yes	
Wallet Availability	Phase 01: Yes	Phase 02: Yes	Phase 03: Yes

iGrant.io enables natural persons to participate in trusted digital ecosystems through its Data Wallet, available as a mobile app or a white-label SDK. Designed for integration by any organisation seeking to issue or facilitate an EUDI Wallet, the solution is fully compliant with eIDAS 2.0 and the EU Implementing Acts.

Built on open standards, including OpenID4VCI and OpenID4VP, the wallet supports the issuance, storage, and selective disclosure of W3C verifiable credentials, including those based on SD-JWT and ISO 18013-5 (mobile driving licence, mDL).

With native support for cross-border interoperability with multiple EU language support, SCA, and secure transaction signing, the wallet is also capable of facilitating identity-linked payment authorisations. This was demonstrated in production as part of the EWC payment task force contributions. Individuals retain full control over their credentials, enabling privacy-preserving, consent-based interactions with both public and private sector services. iGrant.io Data Wallet was used in the following key scenarios in the EWC LSP:

- Travel scenario production scenario led by Amadeus, used for Lufthansa flight booking scenarios during EWC Phases 02 and 03.

5.2 Bank-led payment production during EWC Phase 02, as well as merchant-led payment production for buying ferry tickets during EWC Phase 03

- Cross-LSP testing demonstrating interoperability with Potential.

5.1.2 Lissi ID-Wallet

LSP Contributions	Active contributor to the EWC ecosystem enabler track, contributing as authors or reviewers of RFCs [2]. Supported the development of the ITB with feedback.	
Platform Support	iOS: Yes	Android: Yes

Wallet Availability	Phase 01: Yes	Phase 02: Yes	Phase 03: Yes

The Lissi ID-Wallet is a secure digital wallet solution designed for users to receive, store, manage, and present digital credentials. It facilitates seamless digital interaction with organisations and companies.

Key capabilities of the Lissi Wallet include:

Credential Management: Users can receive and securely manage various digital certificates, member cards, employee passes, and licences.

On-Demand Presentation: It allows users to present their credentials as needed to access digital services and establish trusted connections with organisations.

Interoperability: The Lissi EUDI-Wallet Solution is designed for compatibility with ITB and undergoes active testing with available relying parties.

Lissi ID-Wallet is a finalist in the German EUDI Wallet challenge, showcasing an exemplary implementation approach for the German EUDI Wallet, including (Q)EAA issuance and verification, identification via PID and SCA.

5.1.3 Validated ID

LSP Contributions	Active contributor to the EWC ecosystem enabler track, contributing as authors or reviewers of RFCs [2]. Supported the development of the ITB with feedback.		
Platform Support	iOS: Yes	Android: Yes	
Wallet Availability	Phase 01: Yes	Phase 02: Yes	Phase 03: Yes

VIDwallet is a smartphone-based identity wallet that serves as a core component of VIDidentity. Designed for both iOS and Android, it functions as the digital counterpart to a physical wallet, allowing users to securely store and manage their personal information, credentials, identifiers, and cryptographic key material. Users maintain full control over their data, which is stored in an encrypted form and protected by the device's secure element, ensuring tamper-proof storage.

The wallet supports biometric access, multilingual interfaces (Spanish, English, Catalan, and German), and complies with major interoperability and regulatory standards. Additionally, VIDwallet supports OpenID standards and includes features for organising, searching, and managing credentials, reinforcing its role as a secure, user-centric identity management tool.

5.1.4 Digidentity

LSP Contributions	Contributor to the EWC ecosystem enabler track, reviewing RFCs [2]. Supported the development of the ITB.

Platform Support	iOS: NA	Android: NA	
Wallet Availability	Phase 01: No	Phase 02: No	Phase 03: Yes

Designed with user experience at its core, the wallet features intuitive elements, including a credential usage history, customisable cards, and a guided onboarding process that ensures a seamless adoption experience for all users. The application supports 11 languages, including Dutch, English, Spanish, and German, to ensure accessibility and inclusivity across diverse user groups.

Interoperability is built in through support for open standards, such as OpenID4VCI, OpenID4VP, and W3C Verifiable Credentials, as well as credential formats like SD-JWT and mdoc/mDL. The wallet meets the requirements of the EUDIWallet framework. It complies fully with eIDAS 2.0 and related interoperability and regulatory standards, including features for organising, searching, and managing credentials, thereby reinforcing its role as a secure, user-centric identity management tool.

5.1.5 E-Group MyD

LSP Contributions	Contributor to the EWC ecosystem enabler track, reviewing RFCs [2] and participating in discussions.		
Platform Support	iOS: NA	Android: NA	
Wallet Availability	Phase 01: No	Phase 02: No	Phase 03: No

E-Group MyD wallet supports eIDAS-compliant user authentication/identification, attribute/attestation retrieval from authentic, accurate, and up-to-date data sources, signature creation, and the delivery of documents based on GDPR-compliant consent management. The web-based (browser or WebView in mobile application) MyD wallet has been available on the market since 2017. At its first reference customer, MyD supports the automatic electronic contracting (student loan) workflow, starting from a blank template and delivering the filled and mutually signed document. eIDAS 1.0 interfaces already supported the automation of all these steps, but now eIDAS 2.0 interfaces can be accessed as well (which were successfully tested in the EWC LSP).

5.1.6 DVV Wallet

LSP Contributions	Contributor to the EWC ecosystem enabler track, reviewing RFCs [2] and participating in discussions.		
Platform Support	iOS: No	Android: Yes	
Wallet Availability	Phase 01: No	Phase 02: Yes	Phase 03: No

Finnish EUDI Wallet demo wallet app for Android was created to support DVV's participation in EWC, Potential and DC4EU, and to demonstrate DVV's EUDI Wallet status

and capabilities for a natural person user. The wallet app is distributed via Google Play to pre-registered users.

The demo app provides a high-level user experience for supported use cases, which include OpenID4VCI protocol-based issuance of PID or other credentials, such as a mobile driver's license, diploma credential, or Photo ID, and presenting these credentials to verifiers. The wallet supports credentials in both SD-JWT and mdoc format. The presentation protocols OpenID4VP and ISO 18013-5 are supported, and HAIP (OpenID4VC HAIP with SD-JWT VC) are implemented where applicable.

More information on the implemented DVV wallet solution is available here.

5.1.7 Others

In addition to the above wallet providers, others participated during the RFC process and attempted testing against the ITB, including BankID (Sweden), Google Wallet, Triveria (ID Union), InfoCamere (Italy), and DIGG (Sweden).

5.3 Legal Person or Business Wallet Solutions

Organisational Wallet Solution (With Issuer/Holder/Verifier functionalities): The following enterprise offerings were committed and tested for EWC RFC compliance and tested against the ITB. The status is based on EWC Phase 03 use case scenarios (Dated: July 2025).

Enterprise Offering	URL	RFC001	002	003	004	005	006	007	008	010	011	012	013	100
iGrant.io - Organisation Wallet Suite	Link	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
Mini-Wallet	Link	✅	✅	✅										

Table 03: List of Legal Person Wallets or Business Wallets with Issuer / Holder / Relying Party functions compliant with EWC RFCs

Issuer-Only and/or Relying Party/Verifier-only: The following enterprise offerings were committed and tested for EWC RFC compliance and tested against the ITB. The status is based on EWC Phase 03 use case scenarios (Dated: July 2025)

Enterprise Offering	URL	RFC001	002	003	004	005	006	007	008	010	011	012	013	100
VIDidentity Studio	Link	✅	✅	✅		✅				✅				✅
Lissi EUDI Wallet Connector	Link	✅	✅		✅			✅	✅			✅		✅
University of Aegean	[N/A]	✅	✅	✅		✅		✅	✅			✅	✅	✅
SICPA Digital Trust Suite	Link	✅	✅	✅		✅							✅	✅
CZ.NIC	Link	✅	✅	✅	✅									
Digidentity	[N/A]	✅	✅	✅	✅					✅		✅	✅	✅
Amadeus	Link		✅			✅							✅	
Robert Bosch GmbH	Link	✅	✅									✅		✅
Infocert	Link	✅	✅							✅		✅		✅
Signicat	Link	✅	✅							✅		✅		✅

Table 04: List of Issuers-only or Relying Party-only solutions compliant with EWC RFCs

Co-funded by the European Union

5.1.1 iGrant.io Organisation Wallet Suite

The Organisation Wallet by iGrant.io enables organisations to act as issuers, holders, and verifiers of verifiable credentials. It is fully compliant with eIDAS 1.0, as amended by eIDAS 2.0, and the EUDI framework, incorporating the latest Implementing Acts.

Available both as an on-premise deployment and as a platform-as-a-service (PaaS), the solution offers multi-tenant capabilities suitable for large-scale and high-trust environments. It supports a wide range of credential types, including PID, LPID, EAAs, payment wallet attestations and QEAAs, enabling trusted digital identity management across diverse organisational workflows.

Within the EWC, iGrant.io worked closely with Bolagsverket to implement full LPID lifecycle support in a multi-tenant environment (including revocation and WUA), contributed to the payment task force by enabling the first production payment flows with a pluggable payment authenticator module for merchant-led scenarios, and actively supported the formulation and testing of the ITB.

5.1.2 VID Identity Studio

VIDcredentials Studio enables the full lifecycle management of verifiable credentials, including creation, signing, verification, and revocation. It features a web portal for credential issuance and audit tracking, as well as APIs for seamless integration with existing systems.

5.1.3 Lissi EUDI Wallet Connector

The Lissi EUDI Wallet Connector enables organisations to interact with all EUDI Wallets with a stable API interface. The application can be deployed on-premise and enables identification (KYC), issuance, and verification of credentials (EAA, QEAA), as well as strong customer authentication (such as payment approvals) and digital signatures.

5.1.4 Digidentity

Digidentity's enterprise offerings include comprehensive support for the issuance and lifecycle management of verifiable credentials at the organisational level. This encompasses company identity verification, the ability to issue and manage invitations to individuals or entities, and the use of secure digital signatures to ensure the authenticity, integrity, and trustworthiness of issued credentials.

5.1.5 Others

In addition to the above, several other entities contributed during the RFC process, including Infocamere (Issuer), Infocert (Issuer), Intesi Group (Verifier), Signicat (Issuer), Amadeus (Verifier), and RDE (Budacastle verifier).

6. Insights and recommendations

The EWC has taken a pragmatic and structured approach to ensure alignment, interoperability, and regulatory compliance within the EUDI ecosystem. By introducing a collaborative and transparent RFC process, the consortium has successfully bridged the gap between high-level regulatory and architectural requirements and practical, real-world implementations across diverse wallet solution providers.

This deliverable outlined how the RFC process drives technical consensus, reduces fragmentation, and enables consistent and repeatable results in the LSP test environments. With a growing list of wallet solutions and enterprise offerings demonstrating RFC compliance through the ITB, the EWC has laid a scalable foundation for deploying secure and trusted digital identity wallets across Europe.

As the ecosystem continues to evolve, the RFC process will remain essential as both a technical artefact and a living governance instrument that adapts to emerging standards, stakeholder needs and legislative developments. To strengthen and further enable the EUDI Wallet ecosystem, **it is strongly recommended to maintain and continuously update the Interoperability Test Bed**, ensuring it reflects the latest technical and standards requirements, as well as security expectations, and adapts to any regulatory changes. This ongoing effort will help all participants validate solutions more effectively and foster a robust, future-ready environment for European Digital Identity. Continued collaboration and contribution to this process will be key to building a truly interoperable and user-centric European Digital Identity framework.

Co-funded by the European Union

References

[1] European Commission, Architecture and Reference Framework. Available at: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/

[2] EWC RFCs, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs

[3] EWC Deliverable D3.2, “Open-source software, hosting and documentation for the ODI wallets”

[4] EWC Deliverable D4.3 “Interoperability report on Wallet Implementation”

Appendix A: Business Wallet requirement compliance

The table below outlines the compliance of the Business Wallet / Issuer and Verifiers within EWC. Note that these were formulated as part of a survey delivered initially as part D3.2 [3], but have been updated based on discussions during the RFC/ITB processes.

What is the name of your wallet application?	iGrant.io Organisation Wallet	Spherity EIDA	Mini-Wallet	VIDidentity Studio	SICPA DTS Business Wallet	Bosch Organisation Wallet
As a wallet application provider, are you committing to support user authentication aligned with the required Level of Assurance (LoA) defined in the ARF?	Yes	Yes	No	Yes	Yes	Yes
Can authenticated end users view the attestations stored in the wallet application?	Yes	Yes	Yes	Yes	Yes	Yes
Does the wallet application allow authenticated end users to view historical information about expired and/or deleted attestations?	Yes	Yes	Yes	Yes	Yes	Yes
Does the wallet application provide a GUI for end users?	Yes	Yes	Yes	Yes	Yes	No
Can authenticated end users view the presentations that have been requested from their wallet?	Yes	Yes	No	Yes	Yes	No
When requesting an attestation, can authenticated end users view information from the Issuer's PID?	Yes	No	No	Yes	Yes	No
Does the wallet application display the status (e.g., Operational/Valid) of the wallet instance that is requesting a presentation from the end user?	Yes	No	No	No	Yes	Yes

Co-funded by the European Union

Does the wallet application display the status (e.g., Operational/Valid) of the wallet instance that sends attestation responses?	Yes	No	No	No	Yes	Yes
Can the wallet application accept requests and/or events from the wallet core component?	Yes	Yes	Yes	Yes	Yes	Yes
Can the wallet application send requests to the wallet core component?	Yes	Yes	Yes	Yes	Yes	Yes
Can the WCC automatically respond with a presentation of the attestation when requested?	Yes	Yes	Yes	No	No	Yes
Can the WCC automatically respond with a presentation of a WUA when requested?	Yes	No	No	No	No	Yes
Can the WCC store deleted attestations and presentations in a historical log?	Yes	Yes	No	Yes	No	Yes
Can the WCC be installed in different server environments, including cloud-based and/or on-premise setups?	Yes	Yes	Yes	Yes	Yes	Yes
Can WCCs exchange PIDs in an automated way?	Yes	Yes	Yes	No	No	Yes
Can WCCs exchange wallet trust establishments in an automated way?	Yes	No	No	No	No	Yes
Does the WCC offer an interface for fetching one or more decrypted attestations stored in the WCC?	Yes	Yes	No	No	Yes	No

Co-funded by the European Union

Does the WCC offer an interface for fetching transaction logs stored in the WCC?	Yes	Yes	Yes	Yes	No	Yes

Co-funded by the European Union

Appendix B: Summary of key technological choices in EWC

Category	Supported Options
Formats	W3C VC (JWT), IETF SD-JWT, ISO 18013-5 (mdoc, mDL)
Issuance Protocol	OpenID4VCI - Draft 15 (ID2), EWC RFC001: Issue Verifiable Credential - v3.0
Key Managements	JSON Web Key (JWK) via .well-known/jwk_uri, did:key:jwk_jcs-pub, did:web, X.509 certificates based keys
Presentation Protocols	OpenID4VP - Draft 23 (ID3), EWC RFC002: Present Verifiable Credentials - v3.0
Signing Algorithms	ECDSA (secp256r1/P-256) with SHA-256, RS256
Revocation Management	Token Status List
Trust Managements	Verifier known issuer, X.509 certificates, EWC adapted EU Trust List (as per ETSI TS 119 612)

Co-funded by the European Union