Dissemination level: Public

EWC D4.1

Core Interoperability Specification
WP4

Author: SUNET

Contributors: Signicat, iGrant.io, University of the Aegean

Day of submission: 30/04/2025

Contents

Co-funded by the European Union

Revisions

Version	Date	Author	Changes
v 0.1	08.04.2025	SUNET	First version for approval by the EWC Management Board
v1.0	<Fill in date >	SUNET	Final version reviewed and agreed by contributors. Under review of Project Coordinators.
v1.1	24/04/2025	Signicat	Updated according to the agreed changes in the meeting with WP3 and coordinators: • Slight adjustment in the wording of the exec summary • Added a section on the nothing-at-the-beginning and overflow-towards-the-end situation of our project • Added a paragraph on no-ISO-present (well there is some if you look hard enough) • Updated the list of RFCs (omitted full description, replaced by reference listing)

Co-funded by the European Union

Executive Summary

This document describes the interoperability specifications in EWC. It summarises the challenges in the volatile space of evolving specifications, standards and legislations in scope of the EUDI Wallet and the approach taken to achieve the interoperability within EWC while mitigating these challenges. To ensure interoperability within EWC, all wallets, issuer-only, or verifier-only applications must comply with the EWC RFCs, which define the scope of implementation within the project, and complete compliance testing with the EWC Interoperability Test Bed (ITB). This document describes the context of the EWC RFCs and lists all of the referenced standards and specifications.

This deliverable is part of a comprehensive set of deliverables, providing full overview of interoperability specifications and applicability:

- D4.1 Core Interoperability Specification (this document, due date 30/04/2025)
    - Core interoperability specification on standards, protocols and extensions used in our project.
- D4.2 Applicability Statement for each use case (due date 31/05/2025)
    - Document providing an applicability statement for the credentials for each use case, including any extensions.
- D4.3 Interoperability report on wallet implementation (due date 30/06/2025)
    - Report on interoperability on all wallet implementations in our project (and the variations).

Together with deliverables D4.2 and D4.3, it meets Milestone MS13 “Interoperability descriptions finalised".

The information in this document describes the state of affairs in April 2025, while further changes will be part of the EWC Final Technical Report. A full overview on all the wallets and their compliance, as well as full descriptions of the EWC RFCs will be provided in deliverable D3.1 (due date 31/07/2025).

Co-funded by the European Union

List of abbreviations

Acronym	Explanation
(Q)EAA	(Qualified) Electronic Attestation of Attribute
EAA	Non-Qualified Electronic Attestation of Attribute
Pub-EAA	Public Electronic Attestation of Attribute
ACM	Access Control Body Mechanism
ARF	Architecture and Reference Framework
CBOR	Concise Binary Object Representation
CIR	Commission Implementing Regulation
COSE	CBOR Object Signing and Encryption
DTC	Digital Travel Credential
EDIR	European Digital Identity Regulation
eID	electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
ETIAS	European Travel Information and Authorisation System
EUDI	European Digital Identity
F2F	Face-to-Face
FAQ	Frequently Asked Questions
FAR	False Acceptance Rate
ICAO	International Civil Aviation Organization
ISO	International Organization for Standardization
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
MRTD	Machine Readable Travel Documents
NFC	Near Field Communication
PAD	Presentation Attack Detection
PAN	Primary Account Number
PID	Person Identification Data
QC	Qualified Certificate
QES	Qualified Electronic Signatures

Co-funded by the European Union

1. Introduction

WP4 plays an important role as the architectural work package, providing the essential strategic infrastructure that underpins the success of other work packages that deal with implementations. This work package encompasses a broad range of critical areas, including interoperability, comprehensive technical testing, signing and sealing, and numerous other aspects that are vital to the overall project. By addressing these key areas, WP4 ensures that the technical components of the project integrate seamlessly and function cohesively, ultimately contributing to the successful achievement of project objectives.

Task 1 of WP4 aims to establish a comprehensive framework for enabling interoperability within the European Wallet Consortium (EWC) ecosystem. This is achieved through the development of:

- **Core Interoperability Specifications:** These specifications define the fundamental technical and operational requirements for various components within the EWC ecosystem to interact and exchange data effectively.
- **Extensions for Pilot Use Cases:** To support the pilot use cases within the EWC, the core interoperability specifications will be extended. This will ensure that the interoperability framework is tailored to the unique requirements of each use case.
- **Referencing and Scoping Existing Standards and Specifications:** Wherever possible, the task will leverage and reference existing standards and specifications, including the Architectural Reference Framework (ARF), to ensure consistency and alignment with eIDAS regulation and industry standards. To ensure interoperability, specific scopes of applicability of these standards are defined.
- **Addressing Internal and External Interoperability:** The specifications will encompass both internal and external interoperability. Internal interoperability focuses on ensuring seamless communication and data exchange between different wallet implementations and other infrastructure components within the EWC. External interoperability addresses how the EWC ecosystem can interact with other Large-Scale Pilots (LSPs) and support use cases beyond its boundaries. This includes compatibility with wallet and Personal Identity Document (PID) issuing solutions from Member States.

By establishing these core interoperability specifications and addressing both internal and external interoperability, the task lays a foundation for a cohesive and interconnected EWC ecosystem.

1.1 Approach to Interoperability Specifications in EWC

There are a number of challenges to navigate in order to create the interoperability specification for the EUDI wallet ecosystem. Participants in EWC represent diverse wallet providers, attestation issuers, and verifying relying parties, not all of them engaging in the same use cases and interested in the same functionalities. Standards and specifications are subject to ongoing evolution, which can result in compatibility issues and conflicts when all participants are not able to implement them at the same speed. Furthermore, released standards often leave room for interpretation, particularly in implementation details. Use case

Co-funded by the European Union

requirements encompass both core functionalities and specialized features. The majority of scenario stakeholders operate at the functional and business levels, where distinguishing between core/general and specific aspects can be challenging. Consequently, there is a risk of isolated, non-interoperable islands emerging. Additionally, disparate approaches may lead to gaps such as alignment with ARF/IAs without supporting use cases, or full use case support but lacking ARF / IA conformity.

This task is managing this by closely monitoring the release of the relevant standards, ARF and the EUDI wallet Implementing Acts. EWC project members have been engaging with various standardisation bodies throughout the project, including ETSI/CEN, IETF, CSC and OpenID Foundation. The goal was twofold: to follow the development of relevant standards and translate them into requirements for technical implementation following these standards in support of EWC business cases; and secondly, by active participation in these standardisation bodies, to provide feedback on development of new standards and their versions. EWC project members participated in relevant events including IETF meetings, ETSI/CEN workshops providing formal EWC representation etc.

At the start of the project, many standards were not available, very rudimentary and not aligning to each other: the release of the ARF happened much later than expected and legislation wasn't finalised. This forced us to build a foundation based on the pure requirements from the use cases in our consortium, without any guidance on which standards or specifications to work with, other than a very general sketch on the usage of OpenID4VCI for issuance flows and OpenID4VP/SIOPv2 for attestation exchange (with ISO 18013-5 for proximity flows). Since virtually all our use cases handle remote flows, we decided to stick with early drafts of OpenID4VCI/VP and SD-JWT to start working. At that point there were many basic issues not being easily resolved in the area of selective disclosure and the alignment to the VCDM (v1.1 proved unsuitable for SD-JWT and v2.0 not very mature). Focusing on what we did know and not being overly engaged with everything that was still lacking helped us to start implementations, which we managed to extend and improve ever since.

During the last 6 months of the project the output of standards and specifications has changed to an overflow of information: new versions of standards being released every few weeks, 9 new releases on the ARF in the past 2 months alone and 22 draft legislations listing requirements and technical specifications. But even today most of the needed standards are still unavailable for referencing in the legislation.

To address the rapid and potentially breaking changes in these specifications and legislation, in the beginning of the EWC project the approach taken was to on a quarterly basis freeze the stable versions of these specifications that would be then used as a reference release for the EWC project participants. These were specified as the EWC technological focus https://github.com/EWC-consortium/ewc-wiki/wiki/Focus, and promoted during the EWC "Friday Sessions" reserved for EWC tech-talks https://github.com/EWC-consortium/ewc-wiki/wiki/friday-sessions. These are open to all participants and invite relations from the EC and NiScy as well.

However, further clarifications were needed in order to achieve the same interpretation of the standards and legislation. This was addressed by specifying implementation profiles in the EWC RFCs providing a definition of the wallet interfaces and communication, based on

Co-funded by the European Union

existing standards, specifications and legislation. As presented in Figure 1, the protocol standards, ARF, Implementing Acts, Legislation and EWC use cases requirements were taken as an input creating RFCs. RFCs are in turn used by the individual and organisational wallet providers in the EWC pilots.

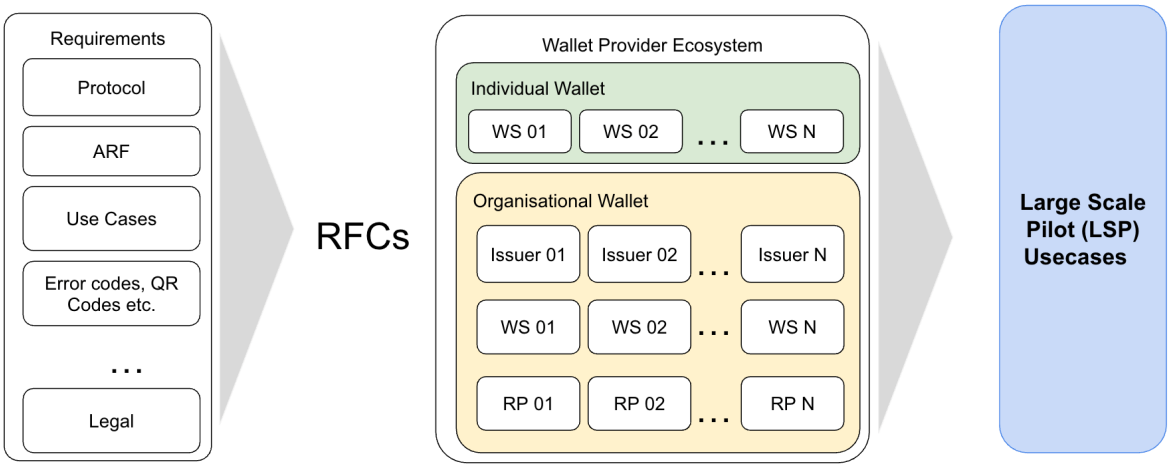

Figure 1: Input for EWC RFCs and their application

The EWC RFCs complement the other specifications needed to support the EWC pilots and the Interoperability Testbed (ITB) which is run within the Task 4.5 and were demonstrated in Deliverable 4.11. This is presented in Figure 2. The Schemas (that define the set of attributes used in an attestation with a specific format) and Rulebooks (that describe the context of a specific set of attestations or data schemas) are further described in Deliverable 4.2. The test scenarios were designed in collaboration with the owners of the use cases in WP2 and WP3 and with the task-leads on signing and issuing in WP4.

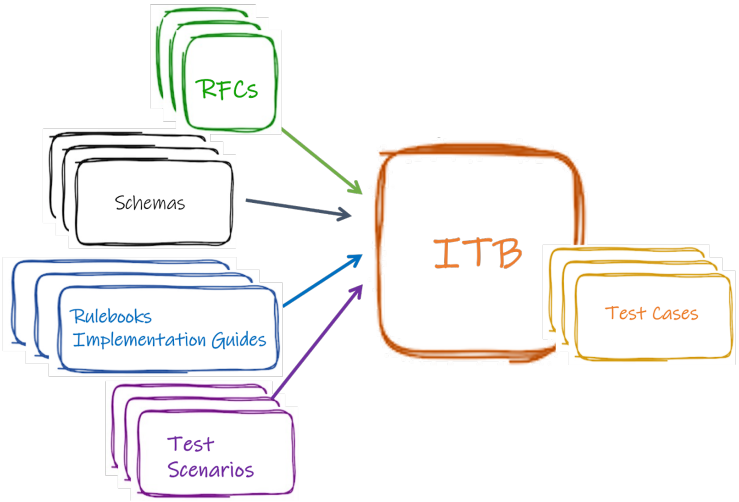

Figure 2: EWC RFC and other scope elements in relation to ITB

Co-funded by the European Union

2. EWC RFCs

EWC RFCs provide descriptions of the interactions of the wallet interfaces with verifiers and issuers. They are based on existing standards, specifications and legislation providing implementation profiles in order to provide clarity on various options and ambiguities and extend them with their own definitions where needed.

To ensure interoperability within EWC, all wallets, issuing and verifying services must comply with the EWC RFC and complete compliance testing with the EWC Interoperability Test Bed (ITB).

This chapter further elaborates on the publishing and naming conventions for the EWC RFCs, release process and dependencies with other specifications used within EWC. A list of the published EWC RFCs and their description is provided in the last part of this chapter.

2.1 Publishing and naming conventions

All EWC RFCs are published in the EWC GitHub, under the https://github.com/EWC-consortium/eudi-wallet-rfcs repository, where:

- Approved EWC RFCs are listed under https://github.com/EWC-consortium/eudi-wallet-rfcs?tab=readme-ov-file#approved-rfcs
- EWC RFCs under development are listed under https://github.com/EWC-consortium/eudi-wallet-rfcs?tab=readme-ov-file#rfcs-under-development

The following naming convection is used:

- RFCs start with `RFC-001-<name-of-the-RFC001-v1.0>`, `RFC-002-<name-of-the-RFC001-v0.9>` etc.
- Name-of-the-RFC should be a comprehensive label describing the RFC.
- The RFC number is assigned within the biweekly RFC/ITB-handling meeting.
- The last part (vX.Y) is the version of the release. Stable versions usually are numbered as full versions (v1, v2) and minor changes typically as decimals (v1.1, v1.2).

2.1.1 Release process

EWC RFC creation and release progress through a collaborative effort and a defined process. Any group within EWC can initiate a creation and propose an EWC RFC following the process described in Figure 3, that can be summarised in following:

- An EWC RFC can be in one of the four lifecycle stages:
  - **Proposed** - A stable version of EWC RFC has been produced, and it is proposed for an approval via the bi-weekly RFC meetings. While working on an EWC RFC Proposal, authors are encouraged to create new RFCs and commit them in a separate branch. Consensus is sought within the EWC community to proceed with at least two entities to co-author as document editors. The community discussions are via EWC Slack #wallet-support group, GitHub issues, PRS, email, etc.

Co-funded by the European Union

- **Candidate** - The EWC RFC is up for review and approval by potential implementors including wallet providers. Consensus is sought from at least two wallet providers, Issuers and/Relying parties within the EWC community to agree to implement the RFC. The community discussions are via EWC Slack #wallet-support group, GitHub issues, PRS, etc. As a result of the review, it can be Approved or Rejected.
- **Approved** - Once agreed upon within the RFC/ITB-handling meetings, a PR for merger to the main branch needs to be raised for an approved EWC RFC. Approved RFCs are then maintained through a release process resolving dependencies as described in the following chapter.
- **Rejected** - Based on received feedback, EWC RFC need to go through revision in order to become Candidate again.

- It might be necessary to maintain different versions (with different version numbers) when new releases of a EWC RFCs are published. This can be a temporary situation, where the old version is removed after all the other elements are updated, or a more permanent situation where use cases or test cases need to be able to use multiple versions.
- Issues can be raised and discussed through GitHub, where all participants in EWC are invited to do so.
- Changes and releases are discussed in biweekly RFC/ITB-handling meetings. This includes current status, raised issues and approval of changes. For ongoing collaboration, guidance and support, the `#wallet-support` channel in the EWC Slack Workspace is used.
- After an EWC RFC or its new version has been approved, it is incorporated into the EWC ITB and test use cases.
- RFC100 defines a general interoperability profile towards the ITB.

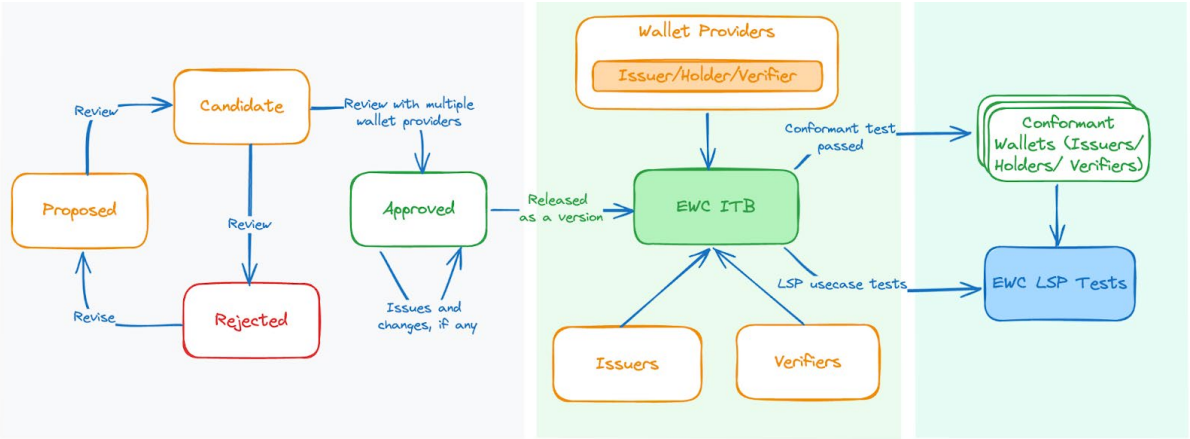

Figure 3: EWC RFC release process

2.2 Dependencies

Before a new version is released, the RFC authors need to validate the dependencies with other EWC scope elements. New versions and releases are taken on in implementations and testing when all these dependencies are resolved, including:

Co-funded by the European Union

- Data schemas - if a RFCs change draws for a different version or require a new data schema.
- Rulebooks - if a RFC changes to the extent that is no longer aligned to the related rulebook(s).

After a new RFC or a change to an existing RFC has been approved, the test cases in the ITB need also to be updated, which may include:

  - For new RFCs either new test cases in ITB need to be implemented and/or existing ones updated.
  - Existing test cases for an RFC need to be updated if the RFC changes. It might be necessary to maintain different versions of an RFC until the test cases are updated (and phased out).

2.2.1 Standards and Specifications referenced in EWC RFCs

For the finalisation of our project, we are working towards a final technical scope and will freeze this to allow for full interoperability testing with all participants. This freeze is planned for mid-May and we expect all EWC RFCs to be based on these core standards and specifications:

- ARF 1.8.0
- OpenID4VCI spec Draft 15 (ID2)
- OpenID4VP Draft 23 (ID3)

Some of the RFCs don't yet use the noted versions of these specifications, but there is a plan to update the RFCs to reflect them. Also, some RFCs might deviate from this if they support a specific use case that has other requirements.

The full list of the standards and specifications referenced in the EWC RFCs is as follows:

- OpenID Foundation, OpenID for Verifiable Credential Issuance
- OpenID Foundation, OpenID for Verifiable Presentations
- OpenID Foundation, 'Self-Issued OpenID Provider v2 (SIOP v2)'
- OpenID4VC High Assurance Interoperability Profile with SD-JWT VC
- IETF, RFC 9396, OAuth 2.0 Rich Authorization Requests
- IETF, OAuth 2.0 Attestation-Based Client Authentication
- IETF, RFC 7591, OAuth 2.0 Dynamic Client Registration Protocol
- IETF, RFC 9449, OAuth 2.0 Demonstrating Proof of Possession (DPoP)
- IETF, RFC 9101, OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR)
- IETF, RFC 7571, JSON Web Key
- IETF, RFC 7636, Proof Key for Code Exchange by OAuth Public Clients,
- IETF, RFC 9126, OAuth 2.0 Pushed Authorization Requests
- IETF, Attestation based client identification
- IETF, Token Status List
- IETF, RFC 7591, OAuth 2.0 Dynamic Client Registration Protocol
- European Commission, The European Digital Identity Wallet Architecture and Reference Framework
- European Commission. Commission Implementing Regulation (EU) 2024/2979 of 2024 on the technical specifications and procedures for ensuring the integrity and

Co-funded by the European Union

core functionalities of the European Digital Identity Wallet under Regulation (EU) 910/2014 of the European Parliament and of the Council
- Implementing Act 2024/2977
- ETSI 119 471
- ETSI TS 119 432
- ETSI TS 119 612
- IANA JWT claim registry
- Cloud Signature Consortium API Specification
- ISO/IEC TS 23220-4 (E) Annex C
- ISO/IEC 18013-5

Note that the standards needed for proximity flows are lacking in this list. As described in our approach, we started working with the requirements for the remote flows based on OpenID4VCI/VP and built the implementations from there. During the project, all use cases proved to be able to work with this setup and stated no urgent need for ISO 18013-5 (or the drafts on 18013-7 with mdoc) to be implemented. As the updates on the earlier chosen standards, along with the vast flow of updates on other requirements from legislation and ARF required most of the resources from implementing participants, it was decided not to incorporate further standards in the EWC RFC. Other priorities on supporting functionalities (e.g. in supporting DC APIs, wallet unit attestations for organisational wallets and incorporating a trust infrastructure) were assigned higher priorities.

2.3 List of EWC RFCs and their referenced standards

A current overview of all EWC RFCs can be found here: https://github.com/EWC-consortium/eudi-wallet-rfcs

Number	RFC-001
Name	Issue Verifiable Credential
Version	V2.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc001-issue-verifiable-credential.md
Reference	1. OpenID Foundation (2023), 'OpenID for Verifiable Credential Issuance', Available at: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.html (Accessed: July 11, 2024). 2. European Commission (2023) The European Digital Identity Wallet Architecture and Reference Framework (2023-04, v1.1.0) [Online]. Available at: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases (Accessed: October 16, 2023). 3. OpenID Foundation (2023), 'Self-Issued OpenID Provider v2 (SIOP v2)', Available at: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html (Accessed: October 01, 2023) 4. OAuth 2.0 Rich Authorization Requests, Available at: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-rar-

Co-funded by the European Union

	11 (Accessed: February 01, 2024) 5. Proof Key for Code Exchange by OAuth Public Clients, Available at: https://datatracker.ietf.org/doc/html/rfc7636 (Accessed: February 01, 2024) 6. OpenID4VC High Assurance Interoperability Profile with SD-JWT VC - draft 00, Available at https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-sd-jwt-vc-1_0.html (Accessed: February 16, 2024) 7. Lodderstedt, T., Campbell, B., Sakimura, N., Tonge, D., and F. Skokan, "OAuth 2.0 Pushed Authorization Requests", RFC 9126, DOI 10.17487/RFC9126, September 2021, https://www.rfc-editor.org/info/rfc9126.

Number	RFC-002
Name	Present Verifiable Credentials
Version	V2.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc002-present-verifiable-credentials.md
Reference	1. OpenID Foundation (2023), 'OpenID for Verifiable Presentations (OID4VP)', Available at: https://openid.net/specs/openid-4-verifiable-presentations-1_0-ID2.html (Accessed: February 1, 2024). 2. European Commission (2023) The European Digital Identity Wallet Architecture and Reference Framework (2023-04, v1.1.0) [Online]. Available at: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases (Accessed: October 16, 2023). 3. RFC 9101 OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR) https://www.rfc-editor.org/rfc/rfc9101.html#name-request-using-the-request_u (Accessed: February 05, 2024) 4. DIF Presentation Exchange: https://identity.foundation/presentation-exchange (Accessed: February 07, 2024)

Number	RFC-003
Name	Issue Person Identification Data (PID)
Version	V2.1
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc003-issue-person-identification-data.md

Co-funded by the European Union

Reference	1. .OpenID Foundation (2024), 'OpenID for Verifiable Credential Issuance (OID4VCI)', Available at: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.html (Accessed: October 10, 2024). 2. European Commission (2025) The European Digital Identity Wallet Architecture and Reference Framework (2025-02, v1.5.1) [Online]. Available at: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases (Accessed: February 10, 2025). Detail of Annex regarding PID issuance is available at: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/annexes/annex-3/annex-3.01-pid-rulebook.md 3. OAuth 2.0 Rich Authorization Requests, Available at: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-rar-11 (Accessed: February 01, 2024) 4. Proof Key for Code Exchange by OAuth Public Clients, Available at: https://datatracker.ietf.org/doc/html/rfc7636 (Accessed: February 01, 2024) 5. OpenID4VC High Assurance Interoperability Profile with SD-JWT VC - draft 1.0, Available at https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-sd-jwt-vc-1_0.html (Accessed: February 16, 2024) 6. Implementing Act 2024/2977, Available at http://data.europa.eu/eli/reg_impl/2024/2977/oj 7. RFC004 for wallet authentication, Available at https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc004-individual-wallet-attestation.md 8. ETSI 119.471 v 0.0.11 [https://docbox.etsi.org/esi/Open/Latest_Drafts/ETSI%20DRAFT%20TS_119_471v0.0.11-public.pdf] (https://docbox.etsi.org/esi/Open/Latest_Drafts/ETSI%20DRAFT%20TS_119_471v0.0.11-public.pdf) 9. IANA JWT claim registry https://www.iana.org/assignments/jwt/jwt.xhtml 10. ARF tech specification for Provider Info https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/technical-specifications/ts2-notification-publication-provider-information.md 11. IETF Attestation based client identification https://datatracker.ietf.org/doc/draft-ietf-oauth-attestation-based-client-auth/

Number	RFC-004
Name	Individual Wallet Unit Attestation
Version	v1.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc004-individual-wallet-attestation.md

Co-funded by the European Union

Reference	[1] European Commission. (2023). The European Digital Identity Wallet Architecture and Reference Framework (ARF). Available at: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework (Accessed: 15-Nov-2024) [2] European Commission. (2023). Commission Implementing Regulation (EU) 2023/XXXX of 2023 on the technical specifications and procedures for ensuring the integrity and core functionalities of the European Digital Identity Wallet under Regulation (EU) 910/2014 of the European Parliament and of the Council. [3] OAuth 2.0 Attestation-Based Client Authentication Draft 03, Available at: https://www.ietf.org/archive/id/draft-ietf-oauth-attestation-based-client-auth-03.html (Accessed: 17-June-2024) [4] Token Status List, Available at: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-status-list-02 (Accessed: 17-June-2024) [5] RFC 7571 JSON Web Key, Available at: https://datatracker.ietf.org/doc/html/rfc7517#section-5 (Accessed: 17-June-2024) [6] OpenID High Assurance Interoperability Profile, Available at: https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-sd-jwt-vc-1_0.html#section-4.3 (Accessed: 17-June-2024) [7] RFC 9449 OAuth 2.0 Demonstrating Proof of Possession (DPoP), Available at: https://www.rfc-editor.org/rfc/rfc9449.html (Accessed: 17-June-2024) [8] EWC RFC001: Issue Verifiable Credential - v2.0, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc001-issue-verifiable-credential.md (Accessed: 17-June-2024)

Number	RFC-005
Name	Issue Legal Identification Data (LPID)
Version	v1.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc005-issue-legal-person-identification-data.md
Reference	1. OpenID Foundation (2023), 'OpenID for Verifiable Credential Issuance (OID4VCI)', Available at: [https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html]) (Published: February 8, 2024). 2. European Commission (2023) The European Digital Identity Wallet Architecture and Reference Framework (2024-04, v1.3.0) [Online]. Available at: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases (Accessed: May 14, 2024). 3. OpenID Foundation (2023), 'Self-Issued OpenID Provider v2 (SIOP v2)', Available at: [https://openid.net/specs/openid-connect-self-issued-v2-1_0.html]) (Published: November 28, 2023) 4. OAuth 2.0 Rich Authorization Requests, Available at: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-rar-11 (Accessed: February 01, 2024)

Co-funded by the European Union

	5. Proof Key for Code Exchange by OAuth Public Clients, Available at: https://datatracker.ietf.org/doc/html/rfc7636 (Accessed: February 01, 2024) 6. OpenID4VC High Assurance Interoperability Profile with SD-JWT VC - draft 00, Available at https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-sd-jwt-vc-1_0.html (Accessed: February 16, 2024) 7. Definition of wallet solution, [https://github.com/malinnorlander/eudi-wallet-rfcs/blob/main/images/Concept%20model.png], as defined in EWC. 8. eIDAS2, add online resource. 9. The JavaScript Object Notation (JSON) Data Interchange Format https://datatracker.ietf.org/doc/html/rfc8259 10. Date and Time on the Internet: Timestamps https://www.rfc-editor.org/rfc/rfc3339 11. JSON Schema https://json-schema.org/

Number	RFC-006
Name	Organisational Wallet Unit Attestation
Version	v1.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc006-organisational-wallet-unit-attestation.md
Reference	[1] EWC RFC001: Issue Verifiable Credential - v2.0, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc001-issue-verifiable-credential.md (Accessed: 11-Dec-2024) [2] EWC RFC002: Present Verifiable Credentials, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc002-present-verifiable-credentials.md (Accessed: 13-Dec-2024) [3] European Commission. (2023). The European Digital Identity Wallet Architecture and Reference Framework (ARF). Available at: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework (Accessed: 15-Nov-2024) [4] European Commission. (2023). Commission Implementing Regulation (EU) 2024/2979 of 2023 on the technical specifications and procedures for ensuring the integrity and core functionalities of the European Digital Identity Wallet under Regulation (EU) 910/2014 of the European Parliament and of the Council, Available at: https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj [5] OAuth 2.0 Attestation-Based Client Authentication Draft 03, Available at: https://www.ietf.org/archive/id/draft-ietf-oauth-attestation-based-client-auth-03.html (Accessed: 17-June-2024) [6] Token Status List, Available at: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-status-list-02 (Accessed: 17-June-2024) [7] OpenID High Assurance Interoperability Profile, Available at: https://openid.net/specs/openid4vc-high-assurance-interoperability-

Co-funded by the European Union

	profile-sd-jwt-vc-1_0.html#section-4.3 (Accessed: 17-June-2024) [8] RFC 7571 JSON Web Key, Available at: https://datatracker.ietf.org/doc/html/rfc7517#section-5 (Accessed: 17-June-2024) [9] RFC 9449 OAuth 2.0 Demonstrating Proof of Possession (DPoP), Available at: https://www.rfc-editor.org/rfc/rfc9449.html (Accessed: 17-June-2024) [10] EWC RFC002: Present Verifiable Credentials - v1.0. Accessible from: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc002-present-verifiable-credentials.md (Accessed: 2024/10/24)

Number	RFC-007
Name	Payment Wallet Attestation
Version	v1.1
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/payment-rfcs/ewc-rfc007-payment-wallet-attestation.md
Reference	1. SCA for online payments using the EUDI Wallet - Implementation guide - v1.01, Available at: [https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/payment-rfcs/implementation-guides/payment-authentication-sca-using-eudi-wallets.pdf] /Accessed: January 3, 2025). 2. EWC RFC001, Issue Verifiable Credential - v1.0, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc001-issue-verifiable-credential.md (Accessed: April 20, 2024). 3. eIDAS2 regulation, Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_EN.pdf (Accessed: April 20, 2024). 4. OpenID4VC High Assurance Interoperability Profile with SD-JWT VC - draft 00, Available at https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-sd-jwt-vc-1_0.html (Accessed: April 10, 2024) 5. EWC RFC004, Individual Wallet Instance attestation, Available at xxx (TBC) (Accessed: April 10, 2024) 6. DIF Presentation Exchange: https://identity.foundation/presentation-exchange (Accessed: April 20, 2024) 7. EWC RFC002: Present Verifiable Credentials - v1.0, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc002-present-verifiable-credentials.md (Accessed, April 20, 2024) 8. OAuth 2.0 Attestation-Based Client Authentication, Available at: https://www.ietf.org/archive/id/draft-ietf-oauth-attestation-based-client-auth-02.html (Accessed: 20-Apr-2024)

Co-funded by the European Union

Number	RFC-008
Name	Payment Data Confirmation
Version	v1.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/payment-rfcs/ewc-rfc008-payment-data-confirmation.md
Reference	1. EMV 3-D Secure overview. Available at: https://www.emvco.com/emv-technologies/3-d-secure/ (Last Accessed: 15 Nov, 2024) 2. Berlin Group overview. Available at: https://www.berlin-group.org/ (Last Accessed: 15 Nov, 2024) 3. EWC RFC 002: Present Verifiable Credentials - v1.0. Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc002-present-verifiable-credentials.md (Last Accessed: 10 Nov, 2024) 4. OpenID for Verifiable Presentations - draft 22. Available at: https://openid.net/specs/openid-4-verifiable-presentations-1_0-22.html (Last Accessed: 10 Nov 2024) 5. EWC RFC 007: Payment Wallet Attestation - v1.0. Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/payment-rfcs/ewc-rfc007-payment-wallet-attestation.md (Last Accessed: 10 Nov, 2024) 6. EWC: Payment Authentication (SCA) using EU DI Wallets – Implementation Guide. Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/tree/main/payment-rfcs/implementation-guides (Last Accessed: 15 Nov, 2024) 7. European Parliament and Council, 2024. Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union, L 1183, pp. 1–45. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401183#d1e38-1-1 (Last Accessed: 15 Nov, 2024) 8. European Parliament and Council, 2015. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Official Journal of the European Union, L 337, 23.12.2015, p. 35–127. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366 (Last Accessed: 15 Nov, 2024) 9. W3C: Payment Request API, Editor's Draft 09 September 2024. Available at: https://w3c.github.io/payment-request/#paymentcurrencyamount-dictionary (Last accessed: 18 Nov 2024) 10. EWC RFC 004: Individual Wallet Unit Attestation - v1.0. Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc004-individual-wallet-attestation.md (Last Accessed: 18 Nov, 2024)

Co-funded by the European Union

Number	RFC-010
Name	Document Signing on a Remote Signing Service Provider using Long-Term Certificates
Version	v1.1
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc010-long-term-certifice-qes-creation.md
Reference	1. OpenID Foundation (2023), 'OpenID for Verifiable Presentations (OID4VP)', Available at: https://openid.net/specs/openid-4-verifiable-presentations-1_0-ID2.html 2. European Commission (2025) The European Digital Identity Wallet Architecture and Reference Framework (2025-02, v1.5.1) [Online]. Available at: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases 3. Cloud Signature Consortium API Specification v2 (2023), Available at: https://cloudsignatureconsortium.org/wp-content/uploads/2023/04/csc-api-v2.0.0.2.pdf 4. ETSI TS 119 432 V1.2.1 (2020), Available at: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf 5. OID4VP v24 https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-new-parameters 6. Proposal for transaction data OID4VP https://docs.google.com/document/d/1E_UlB3fh9zbWiPrzFThEnt69hYN60CWk/edit?tab=t.0

Number	RFC-012
Name	Trust Mechanism
Version	v1.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc012-trust-mechanism.md
Reference	1. ETSI TS 119 612 v2.3.1, Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists, https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.03.01_60/ts_119612v020301p.pdf 2. Trusted List Manager for non-EU countries, available at https://ec.europa.eu/digital-building-blocks/sites/display/TLSO/Trusted+List+Manager+non-EU 3. EWC RFC001, Issue Verifiable Credential - v1.0, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc001-issue-verifiable-

Co-funded by the European Union

	credential.md (Accessed: 23-January, 2025). 4. OpenID Foundation (2023) *OpenID for Verifiable Credential Issuance 1.0 - Draft 1*. Available at: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.htm (Accessed: 23-January, 2025) 5. EWC RFC004, Individual Wallet Unit Attestation - v1.0, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc004-individual-wallet-attestation.md (Accessed: 09-February, 2025) 6. EWC RFC002, Present Verifiable Credential - v1.0, Available at: https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc002-present-verifiable-credentials.md (Accessed: 29-January, 2025) 7. OpenID Foundation, 2023. OpenID for Verifiable Presentations (OpenID4VP) Draft 18. [online] Available at: https://openid.net/specs/openid4vp-18 [Accessed 2 February 2025]. 8. IETF (2015) OAuth 2.0 Dynamic Client Registration Protocol, Available at: https://www.rfc-editor.org/rfc/rfc7591.html#section-2 [The client metadata could be reused] 9. EWC Trust List, 2025, Available at: https://ewc-consortium.github.io/ewc-trust-list/EWC-TL (Accessed: 14, Mar, 2025)

Number	RFC-013
Name	Issuing Photo ID Verifiable Credential
Version	V1.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc013-issue-photoid.md
Reference	1. EUDI Wallet JSON Schema: ds013-photo-id.json 2. ISO/IEC TS 23220-4 (E) Annex C *(2024-08-14)*: Defines the mDoc format for Photo ID. 3. ISO/IEC 18013-5: Specifies mobile driving licenses and digital identity display properties.` 4. OpenID4VCI: Draft Specification.

Number	RFC-100
Name	EWC Interoperability Profile Towards ITB
Version	v2.0
URL	https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc100-interoperability-profile-towards-itb-v1.0.md

Co-funded by the European Union

Reference	1. EWC Technological Focus: https://github.com/EWC-consortium/ewc-wiki/wiki/Focus 2. European Commission's DIGIT Interoperability Testbed https://joinup.ec.europa.eu/collection/interoperability-test-bed-repository/solution/interoperability-test-bed 3. EWC RFC 001: Issue Verifiable Credential - v2.0 https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc001-issue-verifiable-credential.md 4. EWC RFC002: Present Verifiable Credentials - v2.0 https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc002-present-verifiable-credentials.md 5. ITB PDF report 6. ITB XML report

Co-funded by the European Union