Classification: Public

EWC D5.5

Recommendations on Standardisation

WP5

Author: Ministry of Finance, Finland (VM)

Contributors: Annet Steenbergen, Intesi Group, Signicat

Day of submission: 29/07/2025

Contents

Co-funded by
the European Union

Revisions

Version	Date	Author	Changes
v0.1	30/05/2025	Teemu Kääriäinen, VM Annet Steenbergen Viky Manaila, Intesi Group Esther Makaay, Jon Olnes, Signicat	Initial draft version.
v0.2	29/07/2025	SCRO	Reformatted the version that has been approved by the Management Board.

Co-funded by the European Union

Executive Summary

EWC consortium pilots travel-, payment-, and legal person-related use cases in the EUDI wallet ecosystem based on the revised eIDAS Regulation and its Implementing Acts. These provide the high-level guidelines for ecosystem members in different roles to build an interoperable, secure, and privacy-preserving ecosystem of digital identities.

In addition to the Regulation and its Implementing Acts, there is also a need for technical standards to complements their definitions by providing the detailed technical specifications needed to ensure that EUDI wallets can interoperate across borders, that they are secure against evolving threats, and capable of protecting users' privacy by design. They translate high-level legal requirements into consistent, implementable practices that foster trust, compatibility, and innovation within the digital identity ecosystem. Many of these standards are referenced by the Architecture Reference Framework (ARF) and the Implementing Acts. They are developed and defined in various standardisation bodies.

This deliverable covers following topics related to EUDI wallet standardisation activities as part of EWC piloting:

- Identification of standardisation bodies that are relevant for EUDI wallet interoperability, security, and privacy as part of EWC piloting.
- Organisation of liaison activities with relevant standardisation bodies within EWC consortium.
- Identification of relevant standards for EWC piloting.
- Summary of recommendations for identified standards from EWC consortium.

Recommendations from the EWC pilots should significantly enhance the quality, interoperability, security, and privacy of the emerging standards by providing practical insights from real-world implementation. As part of the conducted pilots, the EWC partners have identified gaps, validated assumptions, proposed improvements based on technical and user experience findings, and ensured that standards are fit for purpose, scalable, and aligned with the diverse needs of the EUDI wallet ecosystem.

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 Body Electronic Attestation of Attribute
ACM	Access Control Mechanism
ARF	Architecture and Reference Framework
CBOR	Concise Binary Object Representation
CIR	Commission Implementing Regulation
COSE	CBOR Object Signing and Encryption
CSC	Cloud Signature Consortium
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
ETSI	European Telecommunication Standards Institute
EUDI	European Digital Identity
F2F	Face-to-Face
FAQ	Frequently Asked Questions
FAR	False Acceptance Rate
FRR	False Rejection Rate
IBAN	International Bank Account Number
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

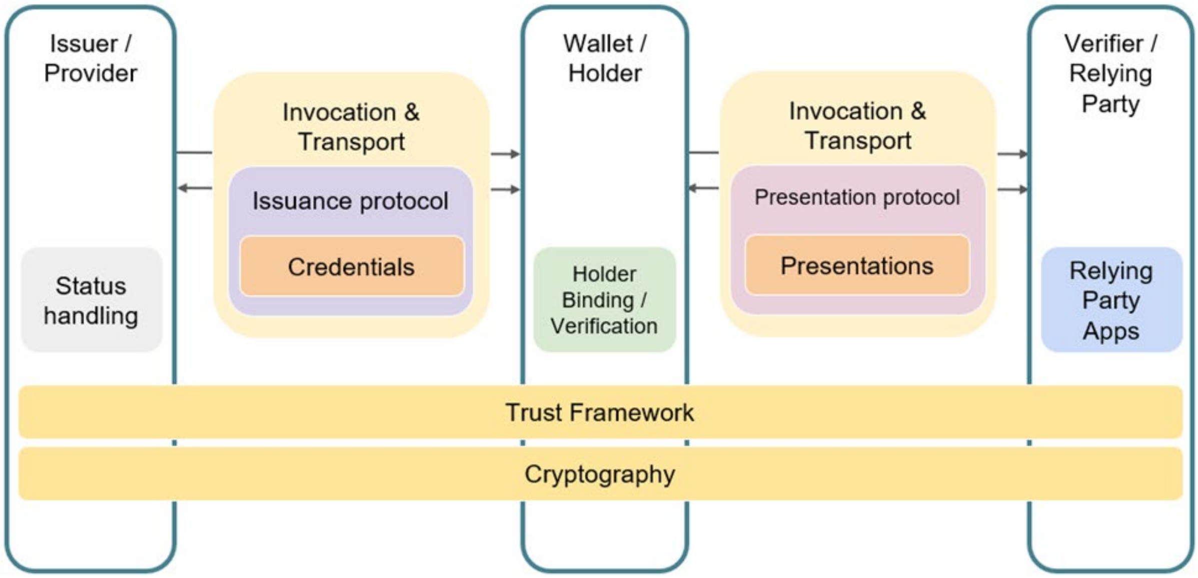
Co-funded by
the European Union

Acronym	Explanation
PAN	Primary Account Number
PID	Person Identification Data
QC	Qualified Certificate
QES	Qualified Electronic Signatures
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
SD-JWT	Selective Disclosure for JWTs (JSON Web Tokens)
SDO	Standards Development Organisation
SOG-IS	Senior Officials Group - Information Systems Security
T&Cs	Terms and Conditions
TSP	Trust Service Provider

1. Introduction

This deliverable details the collaboration activities carried out by the EWC project and its participants with relevant Standards Development Organizations (SDOs). It provides high-level guidance for stakeholders within the EUDI ecosystem across different roles, aimed at fostering the development of interoperable, secure, and privacy-preserving services.

The Wallet ecosystem's standardization landscape is intricate. The picture below, derived from the Global Digital Collaboration event in Geneva, highlights the various layers and functions within the digital credentials stack. Each layer presents multiple standard options, most of which are still in development or undergoing updates. Managing this complexity at EUDI ecosystem level during the implementation and pilot phases of EWC proved challenging. Consequently, continuous monitoring of evolving standards and providing real-world feedback to SDOs were critical activities to support successful deployment.



Source: GDC presentation on standardization for digital credentials

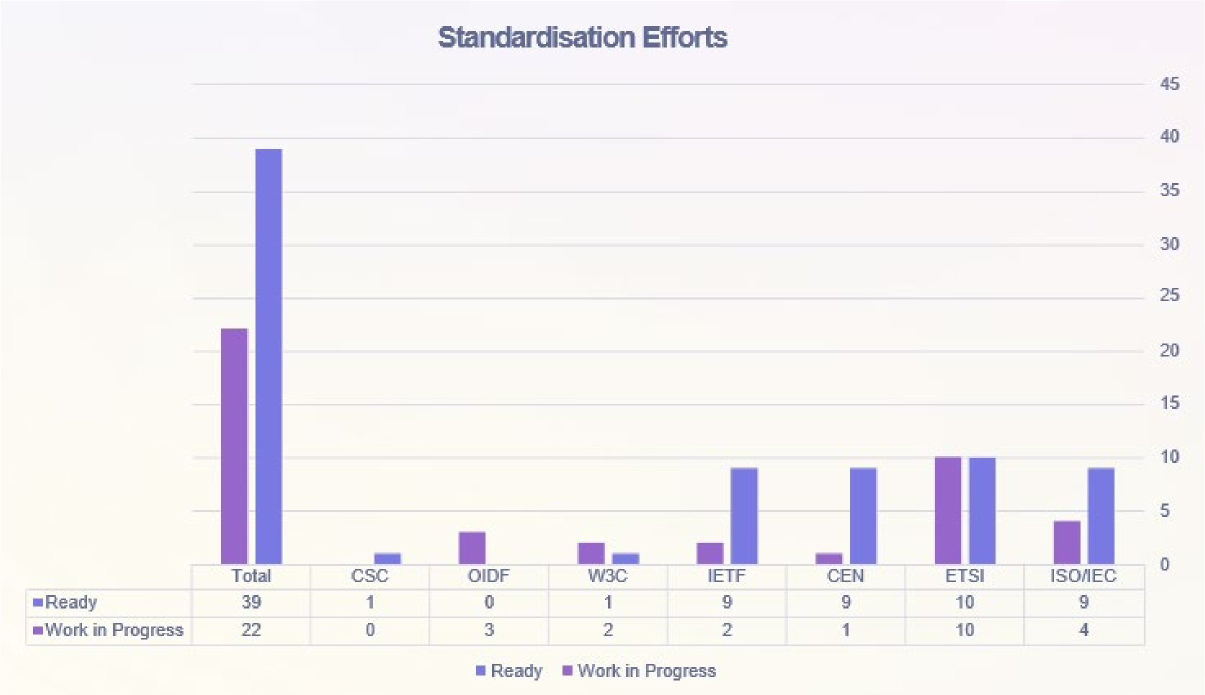
1.1 Purpose of the Deliverable

The European Digital Identity Wallet serves as a vital component of a sophisticated and trustworthy ecosystem. In this interconnected framework, various stakeholders—including wallet providers, personal identification (PID) providers, authentic sources, trust service providers, and relying parties—collaborate seamlessly. This collaboration is designed to facilitate a user-friendly experience for individuals engaging in both domestic and international transactions, ensuring privacy, security and reliability at every step of the process.

The European Commission identified and established the necessary standards and technical specifications to ensure a harmonized and seamless rollout of the EU Digital Identity Wallet across Europe. There are three main categories of relevant organizations:

1. **Recognised European SDOs:** ETSI, CEN/CENELEC
2. **Recognised International SDOs:** ISO/IEC, ITU
3. **Non-recognized SDOs but influential:** W3C, IETF, OpenID Foundation, CSC

Co-funded by the European Union



	Total	CSC	OIDF	W3C	IETF	CEN	ETSI	ISO/IEC
■ Ready	39	1	0	1	9	9	10	9
■ Work in Progress	22	0	3	2	2	1	10	4

Source: EC presentation, September 2024

The complete list of SDOs and their relevant standards and technical specifications is available for detailed consultation here: https://github.com/orgs/eu-digital-identity-wallet/projects/29/views/4

EWC has established robust liaison arrangements with both ETSI (European Telecommunications Standards Institute) and CSC (Cloud Signature Consortium), creating a dynamic and collaborative partnership that ensured a seamless and continuous exchange of information and feedback. This proactive engagement allowed EWC to stay at the forefront of industry developments and directly influence the evolution of standards. Through these established liaisons, EWC actively participates in workshops, ad-hoc meetings, and regular consultations, contributing its expertise and insights during the crucial development phases of new standards. This not only ensures alignment with industry best practices but also facilitates that the resulting standards are comprehensive, relevant, and effectively address the evolving needs of the EUDI framework.

1.2 Scope

The document's scope emphasizes the involvement of established standardization bodies, including domain-specific and other recognized organizations as outlined in D5.4, to ensure that the standards adopted during the pilot phase align with existing best practices and interoperability requirements. During this preparatory phase, particular attention is given to standards that are most relevant for the EWC piloting, especially those that facilitate the issuance of personal identifiers (PID), electronic attestations of attributes, and interactions with relying parties. This focus ensures that the development and testing of digital wallet functionalities are built on a solid foundation of internationally recognized standards, fostering trust and consistency across the pilot environment.

Co-funded by
the European Union

The scope explicitly excludes certain technical areas, such as electronic signing and low-level cryptographic modules, to concentrate on higher-level standards critical for the pilot's success. By doing so, the document aims to focus around core components like PID issuance, attribute attestations, and the interfaces with relying parties, which are central to the EWC's interoperability and usability. This targeted approach ensures that the pilot leverages the most relevant standards to support secure, reliable, and compliant digital identity services, while avoiding scope creep into more technical cryptographic implementations outside the immediate objectives.

1.3 Intended Audience

This deliverable is primarily designed for EWC partners actively involved in the critical tasks of designing and developing the system capabilities of the European Digital Identity (EUDI) Wallet. In addition, this resource is tailored for regulatory, standardization, and certification bodies entrusted with the crucial responsibility of developing relevant standards and ensuring wallet compliance through rigorous auditing and certification processes. These entities will find valuable information to inform their efforts in shaping a secure and interoperable digital identity ecosystem.

Finally, this deliverable is also aimed at privacy and security experts who play a vital role in conducting thorough risk assessments, ensuring robust cybersecurity measures, and guaranteeing privacy assurance throughout the development and deployment of the EUDI Wallet. Their expertise is essential for safeguarding user data and maintaining trust in this critical digital infrastructure.

2. Standardisation Bodies

The European Digital Identity Wallet is a cornerstone of the EU Digital Identity Framework, aiming to provide for all EU citizens an interoperable digital identity solution with privacy and security as central points. As interoperability can be achieved through standards-based services, the European Commission defined a standardisation strategy, engaging with key Standards Development Organisations (SDOs). Key results of this strategy include but is not limited to identification of existing standards and technical specifications necessary for the EUDI Wallet ecosystem, ensure the technical specifications are eligible for reference in the Implementing Acts, highlight missing standards or area where current specifications are not sufficient, address missing technical specifications and engage with relevant bodies to address the gaps.

In an effort to support stakeholders in developing and implementing the necessary services for the EUDI ecosystem, a standardisation roadmap[1] has been made publicly available. It should be noted that alongside the officially recognised EU and international standardisation

[1] https://github.com/orgs/eu-digital-identity-wallet/projects/29/views/2?sliceBy%5Bvalue%5D=ETSI

bodies, there are other standardisation organisations influential by their work and specifications such as OpenID Foundation, W3C, Cloud Signature Consortium or IETF.

The process for referring standards and technical specification in Implementing Acts is governed by the Regulation EU 1025/2012[2]. The regulation primarily emphasizes the role of recognized European Standardization Organizations (ESOs) in developing and referencing standards that support conformity assessment and legal compliance within the EU. However, non-recognized Standard Development Organizations (SDOs) that are influential in their activities can also play a significant role, even if they are not formally recognized under this regulation, and can be referenced in the Implementing Acts.

2.1 CEN/CENELEC

CEN[3] (European Committee for Standardization) and CENELEC[4] (European Committee for Electrotechnical Standardization) play a vital role in the European Digital Identity and Trust Services (EUDI) framework by developing and harmonizing specific standards that underpin secure and interoperable digital identification and trust solutions. They collaborate with other European bodies and standardization organizations to create technical standards for electronic signatures, digital certificates, and trust service providers, ensuring these solutions are legally compliant and technically compatible across all EU member states.

In particular, CEN/TC 224 is responsible for standardisation regarding personal identification and related personal devices with secure elements, systems, operations and privacy in a multi sectorial environment. Relevant for EUDI framework are the following working groups:

Working group	Title	Ongoing or published projects related to EUDI Framework
CEN/TC 224/WG 17	Protection Profiles in the context of SSCD	EN 419241 1 Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements EN 419241 2 Trustworthy Systems Supporting Server Signing Part 2: Protection profile for QSCD for Server Signing

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012R1025

[3] https://www.cencenelec.eu/about-cen/

[4] https://www.cencenelec.eu/

Co-funded by the European Union

Working group	Title	Ongoing or published projects related to EUDI Framework
		Ongoing discussions on common criteria protection profiles for EUDI wallet and protection profile for wallet secure cryptographic application (WSCA
CEN/TC 224/WG 18	Biometrics	prCEN /TS 18099 Biometric data injection attack detection PWI European requirements for biometric products Part 1: General requirements and application profile definition PWI European requirements for biometric products Part 2: Interoperability tests PWI European requirements for biometric products Part 3: Functionality evaluation methodology PWI European requirements for biometric products Part 5: Face biometrics
CEN/TC 224/WG 19	Breeder documents	CEN /TS 17489 2 Secure and interoperable European Breeder Documents Part 2: Data model

Co-funded by the European Union

Working group	Title	Ongoing or published projects related to EUDI Framework
CEN/TC 224/WG 20	European Digital Identity Wallets	CEN /TR 17982 European Digital Identity Wallets standards Gap Analysis prCEN /TS 18098 Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets PWI EUDI Wallet Held Attributes Access Control Potential new project : Guidelines for the Data Management within On Boarded European Digital Identity Wallets

2.2 ETSI

ETSI[5], the European Telecommunications Standards Institute, is an independent, non-profit standards organization focused on developing and defining technical standards for information and communication technologies (ICT) within Europe and globally. ETSI's work supports a wide range of sectors, including telecommunications, cybersecurity, radio, broadcast, and more.

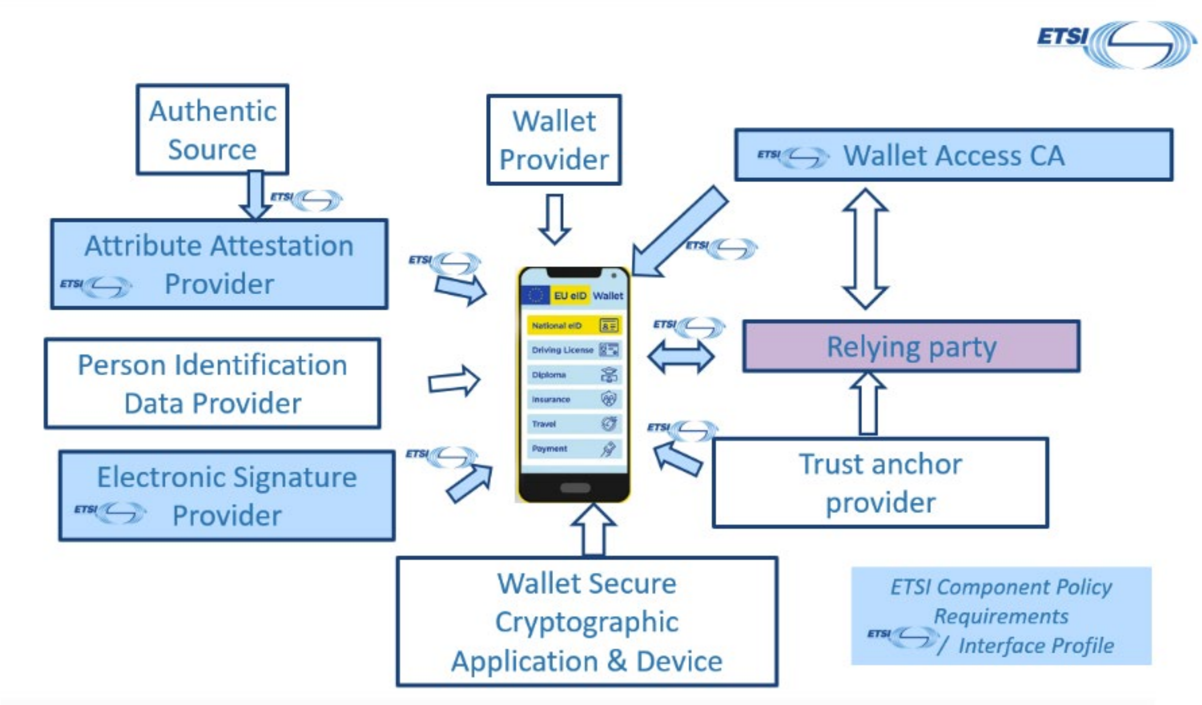
ETSI ESI is the technical committee responsible for developing standards related to electronic signatures, digital certificates, and related trust services. ETSI ESI standards are often aligned with or referenced in European regulations, such as the eIDAS regulation, ensuring compliance with legal requirements. While focused on European needs, ETSI ESI

[5] https://www.etsi.org/

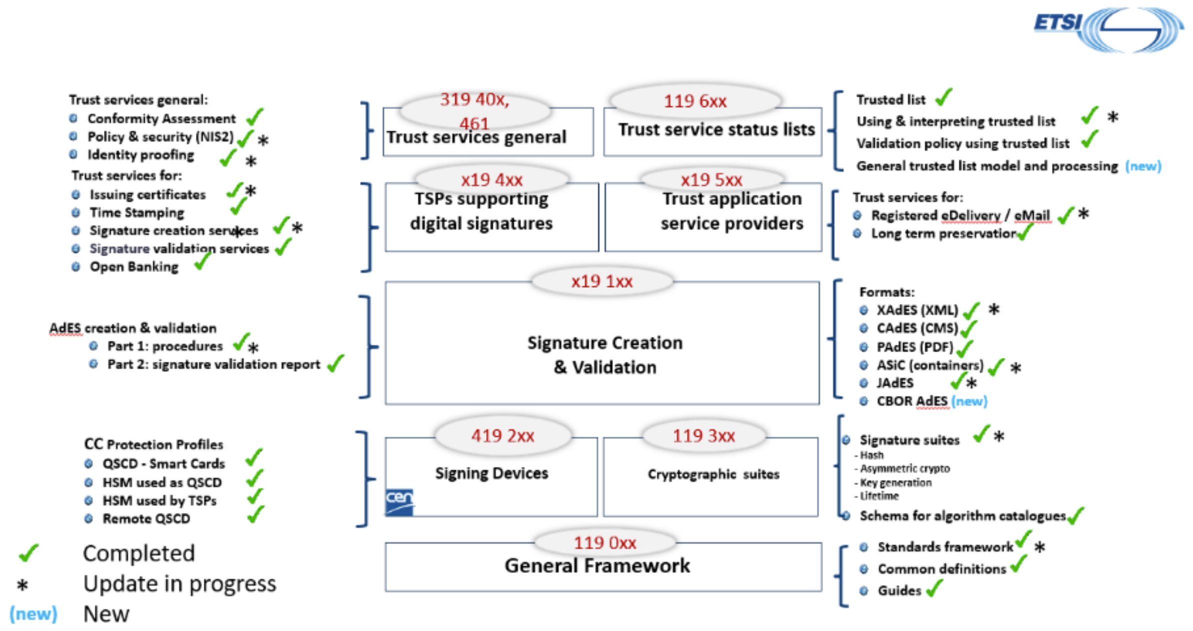
Co-funded by the European Union

standards have significant global influence and are often adopted or adapted in other countries.

The main components and interfaces standardisation for EUDI Wallet under ETSI development are depicted in the figure below:


ETSI
Authentic Source
Wallet Provider
Wallet Access CA
Attribute Attestation Provider
EU eID Wallet
National eID
Driving License
Diploma
Insurance
Travel
Payment
Relying party
Person Identification Data Provider
Trust anchor provider
Electronic Signature Provider
Wallet Secure Cryptographic Application & Device
ETSI Component Policy Requirements / Interface Profile

In addition to the above standards, ETSI maintains and updates existing standards for trust services:



Co-funded by the European Union

2.3 ISO/IEC

The relevant standardization activity for digital identity wallets is carried out by two working groups:

ISO/IEC JTC 1/SC 17/WG 4[6] concentrates on developing generic interfaces and protocols for security devices

ISO/IEC JTC 1/SC 17/WG 10 specifically works on standards related to motor vehicle driver licenses and related documents. This group develops the technical specifications for digital and physical driver licenses, including the data formats, security features, and issuance procedures.

Within the EUDI framework, several ISO/IEC standards play a crucial role in establishing technical interoperability, security, and trust for digital identity wallets. ISO/IEC 18013-5, the foundational standard for mobile driving licences (mDL), provides a generic, hardware-independent solution applicable beyond digital driving credentials, supporting proximity use cases in digital wallets.

This standard is referenced in the Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024, Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 and Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024.

Complementing ISO/IEC 18013-5, ISO/IEC 18013-7 extends the wallet's functionality by introducing additional capabilities such as presenting attestations over the internet and supporting standardized profiles for protocols like OpenID4VP. This standard references draft versions of OpenID4VP and provides a framework for interoperable presentation of verifiable credentials.

This standard is referenced in the Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024.

2.4 Other Standardisation Bodies

Limitations in time and resources didn't allow us to formally engage with all of the standards and standardisation bodies. Therefore we do not report on ITU[7], W3C[8], IETF[9], OpenID Foundation[10], Open Wallet Foundation[11] and Trust over IP[12] in this document. Many of our

[6] https://www.iso.org/committee/45144.html

[7] https://www.itu.int/en/Pages/default.aspx

[8] https://www.w3.org/

[9] https://www.ietf.org/

[10] https://openid.net/foundation/

[11] https://openwallet.foundation/

[12] https://trustoverip.org/

Co-funded by the European Union

members are engaging with these SDOs and have shared information with EWC during the project. Some of these groups have informally requested us to share information with them on various levels of detail and different aspects of our work.

We want to highlight some of the more relevant developments in those SDOs:

OpenID Foundation finalised OpenID4VP to version 1 recently and announced that OpenID4VCI is expected to be finalised in Q3 2025.However, implementers should be aware that this specification relies on several draft standards that are not yet finalized, including OpenID Federation 1.0 draft-43[13], SIOPv2 draft-13[14], SD-JWT draft-22[15], SD-JWT VC draft-09[16], and Fully-Specified Algorithms for JOSE and COSE draft-13[17].

IETF is the SDO for oauth, SD-JWT, JSON and other standards referenced by the ARF. They have created the SPICE working group to aggregate the existing and emerging IETF technologies and address any remaining gaps to facilitate their application in digital credentials and presentations.

The Linux Foundation hosts two relevant projects: The Open Wallet Foundation (OWF) brings developers, standard development organizations and academia together to facilitate global interoperability of verifiable credentials, and The Trust over IP (ToIP) Foundation that provides a robust, common standard and complete architecture for Internet-scale digital trust.

3. Liaison Activities in EWC

In the EWC Consortium, liaison activities are pivotal for fostering collaboration and ensuring alignment with key stakeholders. Viky Manaila from Intesi Group and Jon Ølnes from Signicat have been designated as liaisons to ETSI and the Cloud Signature Consortium (CSC). Their role involves actively participating in relevant working groups and industry events to represent the consortium's interests, contribute to standardization efforts, and stay abreast of evolving technological and regulatory developments. Additionally, they facilitate ongoing communication and cooperation with ETSI and CSC to support interoperability and harmonization of standards and technical specifications suitable for EUDI framework.

The liaisons also serve as the points for feedback collection from consortium partners, ensuring that insights, concerns, and requirements are effectively communicated to the standardisation bodies and consortium members. Within the EWC, Slack is employed as the primary communication channel, enabling real-time exchanges, quick dissemination of

[13] https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html#OpenID.Federation

[14] https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html#SIOPv2

[15] https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html#I-D.ietf-oauth-selective-disclosure-jwt

[16] https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html#I-D.ietf-oauth-sd-jwt-vc

[17] https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html#I-D.ietf-jose-fully-specified-algorithms

information, and coordinated decision-making among participants. The active engagement of the liaisons, combined with constant input from partners, helps drive the successful development and deployment of the EWC project in accordance with relevant standards and ecosystem developments.

While formal liaisons with W3C, IETF, and the OpenID Foundation have not been established, several specifications from these organizations have been integrated into the EWC RFCs to ensure comprehensive interoperability testing among all participants. In particular, Task 4.1 actively monitored the development and evolution of standards and specifications from OpenID and IETF, providing detailed insights and updates within Deliverable D4.1, the Core Interoperability Specification. This approach helped align the ecosystem with current standards and facilitated seamless interoperability across the consortium.

4. Standards for EWC Piloting

The revised eIDAS regulation contains many references to use of standards. The European standards organisations ETSI and CEN consequently initiated work to fill the identified gaps in the standardisation landscape and to revise existing standards in light of the revised eIDAS. ETSI has the responsibility for standards for trust services and related interfaces, while CEN is responsible for standards for EUDI Wallet security.

Below, only the standards of most relevance to EWC are mentioned. Several further ETSI standards are relevant to the EUDI Wallet but considered out of scope of this deliverable, e.g. standards on Trusted Lists, Electronic Registered Delivery services, signature creation, validation and preservation, and conceptual studies on architectures and specific topics such as selective disclosure and zero-knowledge proofs. Some standards are in a too early stage to be considered for EWC piloting, e.g. certificate profiles and requirements for issuing of certificates to actors in the EUDI Wallet ecosystem (wallet providers, (Q)EAA providers, and PID providers).

Similarly for CEN, draft standards in an early stage on security and certification of EUDI Wallets are not considered.

4.1 ETSI TS 119 461 (V2.1.1)

ETSI TS 119 461 is the standard on identity proofing for (qualified) trust services. A new version, v2.1.1, of the standard was developed for the revised eIDAS regulation and published in February 2025. The standard is referenced from the eIDAS Implementing Act on identity verification for qualified certificates and qualified electronic attestation of attributes. Additionally, it is a foundation for the upcoming CEN TS 18098 on onboarding to the EUDI Wallet.

The standard sets policy and security requirements for identity proofing covering physical presence, remote use of identity documents and selfie-video, use of existing eID means, and use of identity from the certificate of a digital signature. Requirements are also set for use of supplementary evidence such as trusted registers (which may be Authentic Sources as defined by eIDAS), documents and attestations (which may be (qualified) electronic

Co-funded by the European Union

attestation of attributes as defined by eIDAS), and proof of possession (e.g. of bank account).

One of EWC's liaisons with ETSI, Jon Ølnes, is ETSI's editor and rapporteur for the standard. Thus, EWC viewpoints have been considered in the work on the standard.

In EWC, the standard is the foundation for work on identity proofing and onboarding in particular for Qualified Trust Service Providers.

4.2 ETSI TS 119 471 (V1.1.1)

ETSI TS 119 471 is the ETSI standard on policy and security requirements for issuers of (qualified) electronic attestation of attributes. The standard was published in its first version, v1.1.1, in May 2025.

The standard sets requirements on operation and management of a service for issuing of (Q)EAA. It is based on the ETSI EN 319 401 standard on basic requirements for (qualified) trust service providers. The standard defines the required security measures that an actor must fulfil notably to issue QEAA.

As this is a foundational standard for this crucial role in the EUDI Wallet ecosystem, EWC submitted consolidated comments on draft versions of the standard, leading to several changes/improvements before the publication.

In EWC, issuing of QEAA is out of scope as the formal audit and supervision regime needed to take this qualified role is not yet in place. However, actors in EWC desiring to take the QEAA issuer role in the future carefully considered the requirements of the ETSI TS 119 471 standard to be prepared for QEAA issuing. In EWC, only non-qualified EAAs were piloted.

4.3 ETSI TS 119 472-1

ETSI TS 119 472-1 is the standard for profiles pertaining to the Electronic Attestation of Attributes (EAA), outlining general requirements. This standard supports the EU Commission Decision "COMMISSION IMPLEMENTING REGULATION (EU) 2024/2977 of 28 November 2024," which establishes rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council concerning personal identification data and electronic attestations of attributes issued to European Digital Identity Wallets.

The document specifies a data model for Electronic Attestations of Attributes, defines requirements for Qualified Electronic Attestations (QEAA) and Public Electronic Attestations (Pub-EAA), and provides realizations for both QEAA and Pub-EAA based on SD-JWT VC, mobile driver's licenses (mDL), W3C standards, and X.509 Attribute Certificates. This standard facilitates selective disclosure of attributes, taking into account the findings of ETSI TS 119 476.

As of the release of stable draft v0.0.7 on June 30, 2025, the EWC participants have not yet utilized this version for defining the EAA profiles.

Co-funded by the European Union

4.4 ETSI TS 119 475 (V0.0.4)

This standard specifies requirements for the use of certificate-based credentials and electronic attestations that support the identification and authorisation of wallet-relying parties when interacting with the European Digital Identity Wallet (EUDIW), in accordance with eIDAS Regulation (EU) No 910/2014, and Commission Implementing Regulation (EU) 2025/848[18] as regards the wallet Relying Party registration.

Specifically, the document defines:

1) policy and profile requirements for **wallet-relying party registration certificates** used to convey the authorisations, entitlements, and intended purposes of wallet-relying parties, as well as the types of attributes they are authorized to request from wallet users;

2) guidance for the inclusion and encoding of wallet-relying party information, such as entitlements, identifiers, and affiliations in both certificates;

3) common requirements for providers of wallet relying party certificates;

4) mechanisms to ensure transparency, security, and user awareness in wallet-based interactions, including mechanisms for attribute minimisation, trust display, and policy alignment.

The specification complements the legal framework established under eIDAS2 for trust service provision, digital identity, and wallet interoperability.

It is currently in the interim draft phase and has not yet been utilized by EWC participants.

4.5 ISO/IEC 23220-4

This document specifies building blocks for the implementation of the operational phase of mobile eID systems and any other mdoc for national bodies or document specific standards to create profiles according to their needs. This document specifies the interface between the mdoc app and mdoc reader and the interface between the mdoc reader and the issuing authority infrastructure. More specifically, it defines transport protocols for various RF solutions and for over the internet. It defines the application layers, such as the request-response protocols between an mdoc app and mdoc reader and between an mdoc reader and issuing authority.

The ISO/IEC 23220 series defines how identity credentials, including Photo IDs, are stored, secured and presented on mobile devices. It uses the mobile driving licence (mDL) as a reference example, which contains a portrait and verified identity attributes. The standard outlines how these attributes are cryptographically bound to the credential and how they can be shared in a privacy-preserving and interoperable manner.

In the EWC these principles have been applied in real-world use cases. The EWC RFC013[19] - Issue PhotoID - defines the implementation of the Annex C of ISO/IES TS

[18] https://eur-lex.europa.eu/eli/reg_impl/2025/848/oj/eng

[19] https://github.com/EWC-consortium/eudi-wallet-rfcs/blob/main/ewc-rfc013-issue-photoid.md#71-iso-23220---photo-id-data-model

Co-funded by the European Union

23220-4 in mdoc and SD-JWT. A Photo ID credential was issued and managed within an EUDI Wallet and successfully used in collaboration with **Amadeus** and **Lufthansa** to support airline processes such as digital check-in. This demonstrated how a Photo ID, built on ISO/IEC 23220 concepts, can be securely shared and verified in a live travel ecosystem.

By aligning with ISO/IEC 23220, implementers of the EUDI Wallet ensure that Photo IDs stored in the wallet are trustworthy, internationally recognised, and ready for seamless use in cross-border services, such as those tested with Amadeus and Lufthansa in the EWC pilots.

4.6 ISO/IEC 18013

The ISO/IEC 18013 series, particularly Parts 5 and 7, provides a strong foundation for mobile identity credentials and has been referenced in the EUDI Wallet Large Scale Pilots. Within these pilots, the European Wallet Consortium (EWC) chose to base its implementations on the ISO/IEC 18013 7 series, as this specification fitted well with the OpenID4VC workflows being tested. ISO 18013 7 defines NFC based and offline presentation methods, enabling secure attribute sharing in proximity use cases such as transport and border control.

These standards are highly relevant because they support privacy preserving data sharing, cryptographic verification and interoperability with existing mobile driving licence ecosystems. By leveraging ISO/IEC 18013 7, the EWC pilots demonstrated how the EUDI Wallet can integrate internationally recognised standards while aligning with emerging credential exchange protocols like OpenID4VC.

It is recommended that EUDI Wallet solutions continue to adopt ISO/IEC 18013 7 as a reference for data structures and exchanges, and extend these methods beyond driving licences to other verifiable attributes. This ensures consistency with eIDAS 2.0 and promotes a trusted and interoperable European Digital Identity Framework.

4.7 prCEN/TS 18098

The prCEN/TS 18098 guidelines is expected to provide a comprehensive framework for onboarding user personal identification data within European Digital Identity Wallets, addressing both online and offline modes of onboarding as outlined in the proposed regulation. This technical specification describes the overall concept and workflow of user onboarding, including the roles and responsibilities of involved parties. It emphasizes the importance of linking the onboarding process to the Level of Assurance (LoA) concept underpinning eIDAS, particularly focusing on meeting the stringent requirements necessary for achieving a "High" LoA as specified in the relevant regulatory annex. The guidelines also aim to encompass various scenarios—such as remote and face-to-face onboarding—offering clear criteria and requirements for each, ensuring interoperability and trust in digital identification procedures across the EU.

Furthermore, the document highlights the qualifications, expertise, and potential accreditation requirements for Conformity Assessment Bodies (CABs) tasked with evaluating and certifying the conformity of user onboarding processes within digital wallets. This ensures that the assessments are conducted by competent entities capable

Co-funded by
the European Union

of verifying that onboarding methods and security measures align with legal and technical standards, particularly for high levels of assurance. Overall, the guidelines aim to facilitate secure, trustworthy, and compliant onboarding processes that support the broader objectives of the European Digital Identity framework, enhancing user confidence and cross-border interoperability.

This technical specification was under development by CEN/TC 224 and the final draft was approved in July 2025. The draft has been provided via the liaison between CEN TC 224 WG 20 and ETSI at the beginning of July, making impossible for EWC participants its consultation and analysis.

4.8 CSC API

The Cloud Signature Consortium[20] develops a standard architecture and API[21] for remote (qualified) signature services, i.e. services that manage private signing keys on behalf of signers. The CSC API is a foundation for the ETSI TS 119 432 standard on APIs for remote signing. ETSI TS 119 431-1 has policy and security requirements for provisioning of remote (qualified) signing.

The CSC API is a REST API to manage signing credentials and invoke signing. It is referenced from an eIDAS Implementing Act and is the foundation for use of remote signing services with the EUDI Wallet. CSC has together with the large-scale pilots worked on revisions to the specification from requirements by eIDAS and in the context of the EUDI Wallet.

Several partners in EWC are contributing members of CSC. Viky Manaila has led the liaison between EWC and CSC and holds the position of President of CSC.

The CSC API is important for all piloting of electronic signatures in EWC, becoming mandatory according to the Commission Implementing Regulation (EU) 2024/2979 regarding integrity and core functionalities of EUDI Wallets . Several actors in EWC provide services according to the CSC API for this piloting. See EWC deliverable D4.7[22] for details on piloting of signing in EWC.

5. Recommendations

To ensure a robust and coherent development of the EUDI Wallet ecosystem, it is essential to enhance clarity, coordination, and inclusiveness within the standardization process. This requires establishing clear distinctions between legal requirements and technical specifications, improving access to relevant standards, fostering early alignment among different stakeholders, and strengthening the involvement of Supervisory Bodies. Addressing these areas proactively will facilitate the development of interoperable, secure, and

[20] https://cloudsignatureconsortium.org/

[21] https://cloudsignatureconsortium.org/resources/download-api-specifications/

[22] https://eudiwalletconsortium.org/wp-content/uploads/2024/11/EWC-D4.8-Overview-and-rationale-for-QES_v1.pdf

Co-funded by the European Union

compliant digital identity solutions that are adaptable to evolving technological and regulatory landscapes. The following recommendations outline key actions to achieve these objectives:

1. **Clarification of the Role and Legal Status of the Architecture and Reference Framework (ARF):**

   It is important to clarify that the ARF serves primarily as a guideline, rather than a legal mandate. Many elements within the ARF are marked as "optional," and it is not a binding legal text. Questions such as whether the support or use of SD-JWT is mandatory should therefore be addressed by distinguishing between legal requirements defined in the implementing regulations and the guidance provided by the ARF. Although future Implementing Acts (IAs) may incorporate specific elements, current understanding must recognize that national policies may override these guidelines, and non-binding recommendations should not be mistaken for obligatory standards.

2. **Access to and Use of ISO/IEC Standards:**

   Given that ISO/IEC standards are not publicly available and require purchase, there is a need for clarity regarding the accessibility of these standards for the purposes of testing and compliance within the consortium. Efforts should be made to explore whether copies can be obtained through collaborative arrangements or other mechanisms, reducing the burden on individual participants. The current situation often results in private sector participants relying on hearsay or bypassing official standards, which can hinder consistent implementation. Addressing this barrier is essential to foster transparency and broad adherence to best practices.

3. **Clear Distinction Between Legal Requirements and Technical Specifications:**

   A structured approach must be adopted to differentiate high-level legal requirements from technical standards and implementation details.

(a) Draft the Implementing Acts (IAs) as high-level legal norms that outline fundamental principles and overarching requirements, allowing flexibility for technical adaptation within the standards.

(b) Ensure that these requirements correspond to current market practices, as implemented by Qualified Trust Service Providers (QTSPs), evaluated by Conformity Assessment Bodies (CABs), and overseen by Member State supervisory authorities. Amendments should adhere to:

- the letter of the eIDAS Regulation;
- the provisions of the ARF;
- and address significant security or interoperability issues, such as recurrent incidents.

4. **Alignment and Coordination Among Standardization Bodies:**

Early and proactive alignment is crucial when multiple groups or organizations are

Co-funded by the European Union

working on the same specifications. Effective coordination should be established from the outset to avoid divergence, enhancing coherence and reducing conflicting technical directions.

5. **Strengthening Involvement of Supervisory Bodies:**

Supervisory Bodies, including CABs and National Accreditation Bodies (NABs), should be more actively engaged in the standardization and certification processes. Their participation is essential to ensure that standards are not only technically sound but also practically enforceable and aligned with regulatory oversight.

6. **Addressing Potential Misalignments Between Legal and Technical Frameworks:**

It is vital to re-examine the alignment between the rapidly evolving legal requirements—such as IAs that may enter into force shortly after publication—and the ongoing development of technical standards under their respective standardization bodies. Particular attention should be given to how updates influence audits and certification processes, ensuring that compliance remains consistent and enforceable throughout the lifecycle of the standards and regulations.

Implementing these recommendations will promote a more coherent, transparent, and effective standardization environment, supporting the secure and interoperable development of the European Digital Identity Wallet ecosystem.

6. Conclusions and Next Steps

Enhancing coordination, clarity, and stakeholder engagement is essential for the successful deployment of the EUDI Wallet ecosystem. Clarifying the distinction between legal and technical frameworks, improving access to standards, and ensuring early alignment among all involved parties will help address current ambiguities.

Next steps include:

- Establishing clear communication on the roles of legal requirements versus standards.
- Exploring shared access mechanisms for ISO/IEC standards.
- Promoting early collaboration among regulators, industry groups, and standardization bodies.
- Increasing involvement of supervisory authorities in certification and oversight.
- Monitoring legal and technical updates to ensure ongoing alignment.

These actions will support a trustworthy, interoperable digital identity ecosystem aligned with EU objectives.

Co-funded by the European Union